Chapter 1
Searching and Seizing Computers Without a Warrant

A. Introduction

The Fourth Amendment limits the ability of government agents to search for and seize evidence without a warrant. This chapter explains the constitutional limits of warrantless searches and seizures in cases involving computers.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

According to the Supreme Court, a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property," *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), and the Court has also characterized the interception of intangible communications as a seizure. *See Berger v. New York*, 388 U.S. 41, 59-60 (1967). Furthermore, the Court has held that a "'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." *Jacobsen*, 466 U.S. at 113. If the government's conduct does not violate a person's "reasonable expectation of privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required. *See Illinois v. Andreas*, 463 U.S. 765, 771 (1983). In addition, a warrantless search that violates a person's reasonable expectation of privacy will nonetheless be constitutional if it falls within an established exception to the warrant requirement. *See Illinois v. Rodriguez*, 497 U.S. 177, 185-86 (1990). Accordingly, investigators must consider two issues when asking whether a government search of a computer requires a warrant. First, does the search violate a reasonable expectation of privacy? And if so, is the

search nonetheless permissible because it falls within an exception to the warrant requirement?

B. The Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers

1. General Principles

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). This inquiry embraces two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *Id.* at 361. In most cases, the difficulty of contesting a defendant's subjective expectation of privacy focuses the analysis on the objective aspect of the *Katz* test, *i.e.*, whether the individual's expectation of privacy was reasonable.

No bright line rule indicates whether an expectation of privacy is constitutionally reasonable. *See O'Connor v. Ortega*, 480 U.S. 709, 715 (1987). For example, the Supreme Court has held that a person has a reasonable expectation of privacy in property located inside a person's home, *see Payton v. New York*, 445 U.S. 573, 589-90 (1980); in "the relative heat of various rooms in the home" revealed through the use of a thermal imager, *see Kyllo v. United States*, 533 U.S. 27, 34-35 (2001); in conversations taking place in an enclosed phone booth, *see Katz*, 389 U.S. at 352; and in the contents of opaque containers, *see United States v. Ross*, 456 U.S. 798, 822-23 (1982). In contrast, a person does not have a reasonable expectation of privacy in activities conducted in open fields, *see Oliver v. United States*, 466 U.S. 170, 177 (1984); in garbage deposited at the outskirts of real property, *see California v. Greenwood*, 486 U.S. 35, 40-41 (1988); or in a stranger's house that the person has entered without the owner's consent in order to commit a theft, *see Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978).

2. Reasonable Expectation of Privacy in Computers as Storage Devices

☞ To determine whether an individual has a reasonable expectation of privacy in information stored in a computer,

> it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer if it would be prohibited from opening a closed container and examining its contents in the same situation.

The most basic Fourth Amendment question in computer cases asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers (or other electronic storage devices) under the individual's control. For example, do individuals have a reasonable expectation of privacy in the contents of their laptop computers, USB drives, or cell phones? If the answer is "yes," then the government ordinarily must obtain a warrant, or fall within an exception to the warrant requirement, before it accesses the information stored inside.

When confronted with this issue, courts have analogized the expectation of privacy in a computer to the expectation of privacy in closed containers such as suitcases, footlockers, or briefcases. Because individuals generally retain a reasonable expectation of privacy in the contents of closed containers, *see United States v. Ross*, 456 U.S. 798, 822-23 (1982), they also generally retain a reasonable expectation of privacy in data held within electronic storage devices. Accordingly, accessing information stored in a computer ordinarily will implicate the owner's reasonable expectation of privacy in the information. *See United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding reasonable expectation of privacy in a personal computer); *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (same); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *United States v. Al-Marri*, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers."); *United States v. Reyes*, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager); *United States v. Lynch*, 908 F. Supp. 284, 287 (D.V.I. 1995) (same); *United States v. Chan*, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (same); *see also United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007) ("A personal computer is often a repository for private information the computer's

owner does not intend to share with others. For most people, their computers are their most private spaces." (internal quotation omitted)).[1]

Although courts have generally agreed that electronic storage devices can be analogized to closed containers, they have reached differing conclusions about whether a computer or other storage device should be classified as a single closed container or whether each individual file stored within a computer or storage device should be treated as a separate closed container. In two cases, the Fifth Circuit determined that a computer disk containing multiple files is a single container for Fourth Amendment purposes. First, in *United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001), in which private parties had searched certain files and found child pornography, the Fifth Circuit held that the police did not exceed the scope of the private search when they examined additional files on any disk that had been, in part, privately searched. Analogizing a disk to a closed container, the court explained that "police do not exceed the private search when they examine more items within a closed container than did the private searchers." *Id.* at 464. In a subsequent case, the Fifth Circuit held that when a warrantless search of a portion of a computer and zip disk had been justified, the defendant no longer retained any reasonable expectation of privacy in the remaining contents of the computer and disk, and thus a comprehensive search by law enforcement personnel did not violate the Fourth Amendment. *See United States v. Slanina*, 283 F.3d 670, 680 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *aff'd*, 359 F.3d 356, 358 (5th Cir. 2004). *See also People v. Emerson*, 766 N.Y.S.2d 482, 488 (N.Y. Sup. Ct. 2003) (adopting intermediate position of treating computer folders rather than individual files as closed containers); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (holding that when a physical ledger contains some information that falls within the scope of a warrant, law enforcement may seize the entire ledger, rather than individual responsive pages).

[1] Although courts have analogized electronic storage devices to closed containers, some courts have also noted characteristics of computers which distinguish them from other closed containers. In *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001), the Tenth Circuit observed that "[t]he advent of the electronic age and . . . the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law." *See also United States v. Stierhoff*, 477 F. Supp. 2d 423, 445 (D.R.I. 2007) ("analogizing a computer file to a closed container is a logical, if not entirely accurate, starting point for addressing the plain view doctrine's application to computer files").

Other appellate courts have treated individual computer files as separate entities, at least in the search warrant context. *See, e.g.*, *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) (approving off-site review of a computer to "separate relevant files from unrelated files"). Similarly, the Tenth Circuit has refused to allow such exhaustive searches of a computer's hard drive in the absence of a warrant or some exception to the warrant requirement. *See United States v. Carey*, 172 F.3d 1268, 1273-75 (10th Cir. 1999) (ruling that agent exceeded the scope of a warrant to search for evidence of drug sales when he "abandoned that search" and instead searched for evidence of child pornography for five hours). In particular, the Tenth Circuit cautioned in a later case that "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer." *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001).

Although individuals generally retain a reasonable expectation of privacy in computers under their control, special circumstances may eliminate that expectation. For example, an individual will not retain a reasonable expectation of privacy in information that the person has made openly available. *See Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *Wilson v. Moreau*, 440 F. Supp. 2d 81, 104 (D.R.I. 2006) (finding no expectation of privacy in documents user stored on computers available for public use in a public library); *United States v. Gines-Perez*, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002) (finding no reasonable expectation of privacy in information placed on the Internet); *United States v. Butler*, 151 F. Supp. 2d 82, 83-84 (D. Me. 2001) (finding no reasonable expectation of privacy in hard drives of shared university computers). Thus, several courts have held that a defendant has no reasonable expectation of privacy in files shared freely with others. *See United States v. King*, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (holding that defendant did not have a legitimate expectation of privacy in the contents of a "shared drive" of his laptop while it was connected to a network); *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007) (holding no reasonable expectation of privacy exists where defendant networked his computer "for the express purpose of sharing files"); *United States v. Stults,* 2007 WL 4284721, at *1 (D. Neb. Dec. 3, 2007) (finding no reasonable expectation of privacy in computer files that the defendant made available using a peer-to-peer file sharing program). Similarly, in *United States v. David*, 756 F. Supp. 1385 (D. Nev. 1991), agents looking over the defendant's shoulder read the

defendant's password from the screen as the defendant typed his password into a handheld computer. The court found no Fourth Amendment violation in obtaining the password because the defendant did not enjoy a reasonable expectation of privacy "in the display that appeared on the screen." *Id.* at 1390. *See also United States v. Gorshkov*, 2001 WL 1024026, at *2 (W.D. Wash. May 23, 2001) (holding that defendant did not have a reasonable expectation of privacy in use of a private computer network when undercover federal agents looked over his shoulder, when he did not own the computer he used, and when he knew that the system administrator could monitor his activities). Nor will individuals generally enjoy a reasonable expectation of privacy in the contents of computers they have stolen or obtained by fraud. *See United States v. Caymen*, 404 F.3d 1196, 1200 (9th Cir. 2005); *United States v. Lyons*, 992 F.2d 1029, 1031-32 (10th Cir. 1993).

3. Reasonable Expectation of Privacy and Third-Party Possession

Individuals who retain a reasonable expectation of privacy in stored electronic information under their control may lose Fourth Amendment protections when they relinquish that control to third parties. For example, an individual may offer a container of electronic information to a third party by bringing a malfunctioning computer to a repair shop or by shipping a floppy diskette in the mail to a friend. Alternatively, a user may transmit information to third parties electronically, such as by sending data across the Internet, or a user may leave information on a shared computer network. When law enforcement agents learn of information possessed by third parties that may provide evidence of a crime, they may wish to inspect it. Whether the Fourth Amendment requires them to obtain a warrant before examining the information depends in part upon whether the third-party possession has eliminated the individual's reasonable expectation of privacy.[2]

To analyze third-party possession issues, it helps first to distinguish between possession by a carrier in the course of transmission to an intended recipient and subsequent possession by the intended recipient. For example, if A hires B to carry a package to C, A's reasonable expectation of privacy in the contents of the package during the time that B carries the package on its way to C may be different than A's reasonable expectation of privacy after C has received the

[2] Regardless of whether an individual retains a reasonable expectation of privacy in an item or information held by a third party, the third party may disclose the item or information to the government provided the third party has common authority over the item or information. *See United States v. Young*, 350 F.3d 1302, 1308-09 (11th Cir. 2003); Section C.1.b, *infra.*

package. During transmission, contents generally retain Fourth Amendment protection. The government ordinarily may not examine the contents of a closed container in the course of transmission without a warrant. Government intrusion and examination of the contents ordinarily violates the reasonable expectation of privacy of both the sender and receiver. *See United States v. Villarreal*, 963 F.2d 770, 774 (5th Cir. 1992). *But see United States v. Young*, 350 F.3d 1302, 1308 (11th Cir. 2003) (holding that Federal Express's terms of service, which allowed it to access customers' packages, eliminated customer's reasonable expectation of privacy in package); *United States v. Walker*, 20 F. Supp. 2d 971, 973-74 (S.D.W.Va. 1998) (concluding that packages sent to an alias in furtherance of a criminal scheme do not support a reasonable expectation of privacy). This rule applies regardless of whether the carrier is owned by the government or a private company. *Compare Ex Parte Jackson*, 96 U.S. (6 Otto) 727, 733 (1877) (public carrier), *with Walter v. United States*, 447 U.S. 649, 651 (1980) (private carrier).

Government acquisition of an intangible electronic signal in the course of transmission may also implicate the Fourth Amendment. *See Berger v. New York*, 388 U.S. 41, 58-60 (1967) (applying the Fourth Amendment to a wire communication in the context of a wiretap). The boundaries of the Fourth Amendment in such cases remain hazy, however, because Congress addressed the Fourth Amendment concerns identified in *Berger* by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2510-2522. Title III, which is discussed fully in Chapter 4, provides a comprehensive statutory framework that regulates real-time monitoring of wire and electronic communications. Its scope encompasses, and in many significant ways exceeds, the protection offered by the Fourth Amendment. *See United States v. Torres*, 751 F.2d 875, 884 (7th Cir. 1984); *Chandler v. United States Army*, 125 F.3d 1296, 1298 (9th Cir. 1997). As a practical matter, then, the monitoring of wire and electronic communications in the course of transmission generally raises many statutory questions, but few constitutional ones. *See generally* Chapter 4.

☞ Individuals lose Fourth Amendment protection in their computer files if they relinquish control of the files.

Ordinarily, once an item has been received by the intended recipient, the sender's reasonable expectation of privacy in the item terminates. *See United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995) (sender's expectation of

privacy in letter "terminates upon delivery"). More generally, the Supreme Court has repeatedly held that the Fourth Amendment is not violated when information revealed to a third party is disclosed by the third party to the government, regardless of any subjective expectation that the third parties will keep the information confidential. For example, in *United States v. Miller*, 425 U.S. 435, 443 (1976), the Court held that the Fourth Amendment does not protect bank account information that account holders divulge to their banks. By placing information under the control of a third party, the Court stated, an account holder assumes the risk that the information will be conveyed to the government. *Id.* According to the Court, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party . . . he cannot object if the third party conveys that information or records thereof to law enforcement authorities"); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (finding no reasonable expectation of privacy in phone numbers dialed by owner of a telephone because act of dialing the number effectively tells the number to the phone company); *Couch v. United States*, 409 U.S. 322, 335 (1973) (holding that government may subpoena accountant for client information given to accountant by client because client retains no reasonable expectation of privacy in information given to accountant).

Courts have applied these principles to electronic communications. For example, in *United States v. Horowitz*, 806 F.2d 1222 (4th Cir. 1986), the defendant emailed confidential pricing information relating to his employer to his employer's competitor. After the FBI searched the competitor's computers and found the pricing information, the defendant claimed that the search violated his Fourth Amendment rights. The Fourth Circuit disagreed, holding that the defendant relinquished his interest in and control over the information by sending it to the competitor for the competitor's future use. *See id.* at 1224-26. *See also Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (stating that sender of email "would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter"); *United States v. Meriwether*, 917 F.2d 955, 959 (6th Cir. 1990) (defendant had no reasonable expectation of privacy in message

sent to a pager); *United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (stating that a sender of an email "cannot be afforded a reasonable expectation of privacy once that message is received.").

Defendants will occasionally raise a Fourth Amendment challenge to the acquisition of account records and subscriber information held by Internet service providers where law enforcement obtained the records using less process than a search warrant. As discussed in Chapter 3.D, the Stored Communications Act permits the government to obtain transactional records with an "articulable facts" court order and specified subscriber information with a subpoena. *See* 18 U.S.C. §§ 2701-2712. These statutory procedures comply with the Fourth Amendment because customers of communication service providers do not have a reasonable expectation of privacy in customer account records maintained by and for the provider's business. *See United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (finding no Fourth Amendment protection for network account holder's basic subscriber information obtained from communication service provider).[3] This rule accords with prior cases finding no Fourth Amendment protection in customer account records. *See, e.g.*, *United States v. Fregoso*, 60 F.3d 1314, 1321 (8th Cir. 1995) (telephone records); *In re Grand Jury Proceedings*, 827 F.2d 301, 302-03 (8th Cir. 1987) (Western Union customer records). Similarly, use of a pen register to capture email to/from address information or Internet Protocol addresses of websites provided to an Internet service provider for routing communications does not implicate the Fourth Amendment. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (email and Internet users have no reasonable expectation of privacy in to/from addresses of their messages or in IP addresses of websites visited).

Although an individual normally loses a reasonable expectation of privacy in an item delivered to a recipient, there is an exception to this rule when the individual can reasonably expect to retain control over the item and its

[3] These cases do not resolve whether an individual maintains a reasonable expectation of privacy in the contents of email in his own email account stored with a provider. *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-08 (9th Cir. 2008) (finding reasonable expectation of privacy in pager messages stored by provider of communication service); *Wilson v. Moreau*, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo! email account).

contents. When a person leaves a package with a third party for temporary safekeeping, for example, she usually retains control of the package and thus retains a reasonable expectation of privacy in its contents. *See, e.g.*, *United States v. James*, 353 F.3d 606, 614 (8th Cir. 2003) (finding that defendant retained Fourth Amendment rights in sealed envelope containing computer disks which he had left with a friend for storage); *United States v. Most*, 876 F.2d 191, 197-98 (D.C. Cir. 1989) (finding reasonable expectation of privacy in contents of plastic bag left with grocery store clerk); *United States v. Barry*, 853 F.2d 1479, 1481-83 (8th Cir. 1988) (finding reasonable expectation of privacy in locked suitcase stored at airport baggage counter); *United States v. Presler*, 610 F.2d 1206, 1213-14 (4th Cir. 1979) (finding reasonable expectation of privacy in locked briefcases stored with defendant's friend for safekeeping).

In some cases, the sender may initially retain a right to control the third party's possession, but may lose that right over time. The general rule is that the sender's Fourth Amendment rights dissipate as the sender's right to control the third party's possession diminishes. For example, in *United States v. Poulsen*, 41 F.3d 1330 (9th Cir. 1994), *overruled on other grounds*, *United States v. W. R. Grace*, 526 F.3d 499 (9th Cir. 2008) (en banc) computer hacker Kevin Poulsen left computer tapes in a locker at a commercial storage facility but neglected to pay rent for the locker. Following a warrantless search of the facility, the government sought to use the tapes against Poulsen. The Ninth Circuit held that the search did not violate Poulsen's reasonable expectation of privacy because under state law Poulsen's failure to pay rent extinguished his right to access the tapes. *See id.* at 1337. *See also United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) ("Once a hotel guest's rental period has expired or been lawfully terminated, the guest does not have a legitimate expectation of privacy in the hotel room." (internal quotation marks omitted)).

4. Private Searches

The Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (internal quotation marks omitted). As a result, no violation of the Fourth Amendment occurs when a private individual acting on his own accord conducts a search and makes the results available to law enforcement. *See id.* According to *Jacobsen*, agents who learn of evidence via a private search can reenact the original private search without violating any reasonable expectation of privacy. What the agents

cannot do without a warrant is "exceed[] the scope of the private search." *Id.* at 115. *See also United States v. Miller*, 152 F.3d 813, 815-16 (8th Cir. 1998); *United States v. Donnes*, 947 F.2d 1430, 1434 (10th Cir. 1991). *But see United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) (stating in dicta that *Jacobsen* does not permit law enforcement to reenact a private search of a private home or residence). This standard requires agents to limit their investigation to the scope of the private search when searching without a warrant after a private search has occurred. Where agents exceed the scope of the private warrantless search, any evidence uncovered may be vulnerable to a motion to suppress.

Private individuals often find contraband or other incriminating evidence on computers and bring that information to law enforcement, and the private search doctrine applies in these cases. In one common scenario, an individual leaves his computer with a repair technician. The technician discovers images of child pornography on the computer, contacts law enforcement, and shows those images to law enforcement. Courts have agreed that such searches by repairmen prior to their contact with law enforcement are private searches and do not implicate the Fourth Amendment. *See United States v. Grimes*, 244 F.3d 375, 383 (5th Cir. 2001); *United States v. Hall*, 142 F.3d 988, 993 (7th Cir. 1998); *United States v. Anderson*, 2007 WL 1121319 at *5-6 (N.D. Ind. Apr. 16, 2007); *United States v. Grant*, 434 F. Supp. 2d 735, 744-45 (D. Neb. 2006); *United States v. Caron*, 2004 WL 438685, at *4-5 (D. Me. Mar. 9, 2004); *see also United States v. Kennedy*, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000) (concluding that searches of defendant's computer over the Internet by an anonymous caller and employees of a private ISP did not violate Fourth Amendment because there was no evidence that the government was involved in the search).

One private search question that arises in computer cases is whether law enforcement agents must limit themselves to only files examined by the repair technician or whether all data on a particular storage device is within the scope of the initial private search. The Fifth Circuit has taken an expansive approach to this question. *See United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001) (police did not exceed the scope of a private search when they examined more files on privately searched disks than had the private searchers). Under this approach, a third-party search of a single file on a computer allows a warrantless search by law enforcement of the computer's entire contents. *See id.* Other courts, however, may not follow the Fifth Circuit's approach and instead rule that government searchers can view only those files whose contents were

revealed in the private search. *See United States v. Barth*, 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998) (holding, in a pre-*Runyan* case, that agents who viewed more files than private searcher exceeded the scope of the private search). Even if courts follow the more restrictive approach, the information gleaned from the private search will often provide the probable cause needed to obtain a warrant for a further search.[4]

Importantly, the fact that the person conducting a search is not a government employee does not always mean that the search is "private" for Fourth Amendment purposes. A search by a private party will be considered a Fourth Amendment government search "if the private party act[s] as an instrument or agent of the Government." *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989). The Supreme Court has offered little guidance on when private conduct can be attributed to the government; the Court has merely stated that this question "necessarily turns on the degree of the Government's participation in the private party's activities, . . . a question that can only be resolved 'in light of all the circumstances.'" *Id.* at 614-15 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971)).

In the absence of a more definitive standard, the various federal Courts of Appeals have adopted a range of approaches for distinguishing between private and government searches. About half of the circuits apply a "totality of the circumstances" approach that examines three factors: whether the government knows of or acquiesces in the intrusive conduct; whether the party performing the search intends to assist law enforcement efforts at the time of the search; and whether the government affirmatively encourages, initiates, or instigates the private action. *See, e.g.*, *United States v. Pervaz,* 118 F.3d 1, 6 (1st Cir. 1997); *United States v. Smythe*, 84 F.3d 1240, 1242-43 (10th Cir. 1996); *United States v. McAllister*, 18 F.3d 1412, 1417-18 (7th Cir. 1994); *United States v. Malbrough*, 922 F.2d 458, 462 (8th Cir. 1990). This test draws a line

[4] After viewing evidence of a crime stored on a computer, agents may need to seize the computer temporarily to ensure the integrity and availability of the evidence before they can obtain a warrant to search the contents of the computer. *See, e.g.*, *Hall*, 142 F.3d at 994-95; *United States v. Grosenheider*, 200 F.3d 321, 330 n.10 (5th Cir. 2000). The Fourth Amendment permits agents to seize a computer temporarily so long as they have probable cause to believe that it contains evidence of a crime, the agents seek a warrant expeditiously, and the duration of the warrantless seizure is not "unreasonable" given the totality of the circumstances. *See Illinois v. McArthur*, 531 U.S. 326, 332-34 (2001); *United States v. Place*, 462 U.S. 696, 701 (1983); *United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998); *United States v. Licata*, 761 F.2d 537, 540-42 (9th Cir. 1985).

between situations where the government is a mere knowing witness to the search and those where the government is an active participant or driving force. However, this line can be difficult to discern. For example, in *United States v. Smith*, 383 F.3d 700 (8th Cir. 2004), police detectives participating in "parcel interdiction" at Federal Express removed a suspicious package from a conveyer belt, submitted it to a canine sniff, and delivered the package to the Federal Express manager, telling the manager that "if she wanted to open it that would be fine." However, because the police did not actually ask or order the manager to open the package, and because there was no evidence that the manager felt obligated to open the package, the Court found that the manager was not a "government agent" for Fourth Amendment purposes. *Id.* at 705. *See also United States v. Momoh*, 427 F.3d 137, 141-42 (1st Cir. 2005) (DHL employee's desire to comply with FAA regulations did not make her a government agent absent "affirmative encouragement"). By contrast, in *United States v. Souza*, 223 F.3d 1197 (10th Cir. 2000), the Court found that a UPS employee was a government agent. In *Souza*, the police identified and removed the package from the conveyer belt, submitted it to a canine sniff, and told the UPS employee that they suspected it contained drugs. The police then told the employee that they could not tell her to open the package, but they pointed to it and said "but there it is on the floor." *Id.* at 1200. The employee began to open the package, but when she had difficulty, the police assisted her. While the officers' actual aid in opening the package made this an easy case, the Court's analysis suggests that the officers' other actions—identifying the package and encouraging the employee to open it—might have made the employee a government agent, particularly without evidence that the employee had an independent motivation to open it. *See id.* at 1202.

Other circuits have adopted more rule-like tests that focus on only the first two factors. *See, e.g.*, *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982) (holding that private action counts as government conduct if, at the time of the search, the government knew of or acquiesced in the intrusive conduct, and the party performing the search intended to assist law enforcement efforts); *United States v. Paige*, 136 F.3d 1012, 1017 (5th Cir. 1998) (same); *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985) (holding that a private individual is a state actor for Fourth Amendment purposes if the police instigated, encouraged, or participated in the search, and the individual engaged in the search with the intent of assisting the police in their investigative efforts).

Two noteworthy private search cases involve an individual who hacked into computers of child pornographers for the purpose of collecting and disclosing evidence of their crimes. The hacker, who refused to identify himself or meet directly with law enforcement, emailed the incriminating evidence to law enforcement. In both cases, the evidence was admissible because when it was gathered, the individual was not an agent of law enforcement. In the first case, *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003), the court had little difficulty in determining that the search did not implicate the Fourth Amendment. Because the relevant searches by the hacker took place before the hacker contacted law enforcement, the hacker was not acting as a government agent, and the private search doctrine applied. *See id.* at 1045. In the *Steiger* case, a law enforcement agent thanked the anonymous hacker, assured him he would not be prosecuted, and expressed willingness to receive other information from him. Approximately a year later (and seven months after his last previous contact with law enforcement), the hacker provided to law enforcement information he had illegally obtained from another child pornographer, which gave rise to *United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003). In *Jarrett*, the court ruled that although "the Government operated close to the line," the contacts in *Steiger* between the hacker and law enforcement did not create an agency relationship that carried forward to *Jarrett*. *Id.* at 346-47. Moreover, although the government created an agency relationship through further contacts with the hacker during the second investigation, that agency relationship arose after the relevant private search and disclosure. *See id.* at 346. Thus, the hacker's private search in *Jarrett* did not violate the Fourth Amendment.

5. Use of Specialized Technology to Obtain Information

The government's use of innovative technology to obtain information about a target can implicate the Fourth Amendment. *See Kyllo v. United States*, 533 U.S. 27 (2001). In *Kyllo*, the Supreme Court held that the warrantless use of a thermal imager to reveal the relative amount of heat released from the various rooms of a suspect's home constituted a search that violated the Fourth Amendment. In particular, the Court held that where law enforcement "uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without a physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40. Whether a technology falls within the scope of the *Kyllo* rule depends on at least two factors. First, the use of technology should not implicate *Kyllo* if the technology is in "general public use," *see id.* at 34, 39 n.6, although courts

have not yet defined the standard for determining whether a given technology meets this requirement. Second, the Supreme Court restricted its holding in *Kyllo* to the use of technology that reveals information about the interior of the home. *See id.* at 40 ("We have said that the Fourth Amendment draws a firm line at the entrance to the house." (internal quotation marks omitted)).

Defendants have occasionally—and unsuccessfully—invoked *Kyllo* in cases in which the government used cell tower information or an electronic device to locate a cell phone. For example, in *United States v. Bermudez*, 2006 WL 3197181 (S.D. Ind. June 30, 2006), *aff'd* 509 F.3d 820 (7th Cir. 2007), the court rejected a *Kyllo* challenge to the use of an electronic device to locate a cell phone because cell phones are used to transmit signals to parties outside a home. In rejecting the defendant's *Kyllo* argument, the court explained that "the cell phone signals were knowingly exposed to a third-party, to wit, the cell phone company." *Id.* at *13.

C. Exceptions to the Warrant Requirement in Cases Involving Computers

Warrantless searches that intrude upon a reasonable expectation of privacy will comply with the Fourth Amendment if they fall within an established exception to the warrant requirement. Cases involving computers often raise questions relating to how these "established" exceptions apply to new technologies.

1. Consent

Agents may search a place or object without a warrant or even probable cause if a person with authority has voluntarily consented to the search. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). The authority to consent may be actual or apparent. *See United States v. Buckner*, 473 F.3d 551, 555 (4th Cir. 2007). The consent may be explicit or implicit. *See United States v. Milian-Rodriguez*, 759 F.2d 1558, 1563-64 (11th Cir. 1985). Whether consent was voluntarily given is a question of fact that the court must decide by considering the totality of the circumstances. While no single aspect controls the result, the Supreme Court has identified the following important factors: the age, education, intelligence, physical and mental condition of the person giving consent; whether the person was under arrest; and whether the person had been advised of his right to refuse consent. *See Schneckloth*, 412 U.S. at 226-

27. The government carries the burden of proving that consent was voluntary. *See United States v. Matlock*, 415 U.S. 164, 177 (1974); *Buckner*, 473 F.3d at 554.

In computer crime cases, two consent issues arise particularly often. First, when does a search exceed the scope of consent? For example, when a target consents to the search of a location, to what extent does the consent authorize the retrieval of information stored in computers at the location? Second, who is the proper party to consent to a search? Do roommates, friends, and parents have the authority to consent to a search of another person's computer files?[5]

Finally, consent to search may be revoked "prior to the time the search is completed." *United States v. Lattimore*, 87 F.3d 647, 651 (4th Cir. 1996) (quoting 3 Wayne R. LaFave, *Search and Seizure* § 8.2(f), at 674 (3d ed. 1996)). When agents obtain consent to remove computers for off-site review and analysis, the time required for review can be substantial. In such cases, law enforcement should keep in mind that before incriminating evidence is found, the consent may be revoked. In cases involving physical documents obtained by consent, courts have allowed the government to keep copies of the documents made by the government prior to the revocation of consent, but they have forced the government to return copies made after consent was revoked. *See Mason v. Pulliam*, 557 F.2d 426, 429 (5th Cir. 1977); *Vaughn v. Baldwin*, 950 F.2d 331, 334 (6th Cir. 1991). There is little reason for courts to distinguish copying paper documents from copying hard drives, and one district court recently stated that a defendant who revoked the consent to search his computer retained no reasonable expectation of privacy in a mirror image copy of his hard drive made by the FBI. *See United States v. Megahed*, 2009 WL 722481, at *3 (M.D. Fla. Mar. 18, 2009).

a. Scope of Consent

"The scope of a consent to search is generally defined by its expressed object, and is limited by the breadth of the consent given." *United States v. Pena*, 143 F.3d 1363, 1368 (10th Cir. 1998) (internal quotation marks omitted). The standard for measuring the scope of consent under the Fourth Amendment is objective reasonableness: "[W]hat would the typical reasonable person have understood by the exchange between the [agent] and the [person granting consent]?" *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). This requires a fact-

[5] Consent by employers and co-employees is discussed separately in the workplace search section of this chapter. *See* Chapter 1.D.

intensive inquiry into whether it was reasonable for the agent to believe that the scope of consent included the items searched. *Id.* Of course, when the limits of the consent are clearly given, either before or during the search, agents must respect these bounds. *See Vaughn v. Baldwin*, 950 F.2d 331, 333-34 (6th Cir. 1991).

Computer cases often raise the question of whether general consent to search a location or item implicitly includes consent to access the memory of electronic storage devices encountered during the search. In such cases, courts look to whether the particular circumstances of the agents' request for consent implicitly or explicitly limited the scope of the search to a particular type, scope, or duration. Because this approach ultimately relies on fact-driven notions of common sense, results reached in published opinions have hinged upon subtle (if not entirely inscrutable) distinctions. *Compare United States v. Reyes*, 922 F. Supp. 818, 834 (S.D.N.Y. 1996) (consent to "look inside" a car included consent to retrieve numbers stored inside pagers found in car's back seat), *with United States v. Blas*, 1990 WL 265179, at *20 (E.D. Wis. Dec. 4, 1990) (consent to "look at" a pager did not include consent to activate pager and retrieve numbers, because looking at pager could be construed to mean "what the device is, or how small it is, or what brand of pager it may be"). *See also United States v. Carey*, 172 F.3d 1268, 1274 (10th Cir. 1999) (reading written consent form extremely narrowly, so that consent to seizure of "any property" under the defendant's control and to "a complete search of the premises and property" at the defendant's address merely permitted the agents to seize the defendant's computer from his apartment, not to search the computer off-site because it was no longer located at the defendant's address); *United States v. Tucker*, 305 F.3d 1193, 1202 (10th Cir. 2002) (allowing computer search pursuant to parole agreement allowing search of "any other property under [defendant's] control"); *United States v. Lemmons*, 282 F.3d 920, 924-25 (7th Cir. 2002) (defendant expanded initial consent to search of cameras and recordings to include computer files when he invited officer to look at computer and failed to object to officer's search for pornographic images). Prosecutors can strengthen their argument that the scope of consent included consent to search electronic storage devices by relying on analogous cases involving closed containers. *See, e.g.*, *United States v. Al-Marri*, 230 F. Supp. 2d 535, 540-41 (S.D.N.Y. 2002) (upholding search of computer in residence and citing principle that separate consent to search closed container in fixed premises is unnecessary); *United States v. Galante*, 1995 WL 507249, at *3 (S.D.N.Y. Aug. 25, 1995) (general consent to search car included consent

to have officer access memory of cellular telephone found in the car, in light of circuit precedent involving closed containers); *Reyes*, 922 F. Supp. at 834.

When agents obtain consent for one reason but then conduct a search for another reason, they should be careful to make sure that the scope of consent encompasses their actual search. For example, in *United States v. Turner*, 169 F.3d 84 (1st Cir. 1999), the First Circuit suppressed images of child pornography found on computers after agents procured the defendant's consent to search his property for other evidence. In *Turner*, detectives searching for physical evidence of an attempted sexual assault obtained written consent to search the defendant's "premises" and "personal property." Before the defendant signed the consent form, the detectives discovered a large knife and blood stains in his apartment, and they explained to him that they were looking for more evidence of the assault that the suspect might have left behind. *See id.* at 85-86. While several agents searched for physical evidence, one detective searched the contents of the defendant's personal computer and discovered stored images of child pornography. The defendant was thereafter charged with possessing child pornography. On interlocutory appeal, the First Circuit held that the search of the computer exceeded the scope of consent and suppressed the evidence. According to the Court, the detectives' statements that they were looking for signs of the assault limited the scope of consent to the kind of physical evidence that an intruder might have left behind. *See id.* at 88. By transforming the search for physical evidence into a search for computer files, the detective exceeded the scope of consent. *See id.*; *see also Carey*, 172 F.3d at 1277 (Baldock, J., concurring) (concluding that agents exceeded scope of consent by searching computer after defendant signed broadly-worded written consent form, because agents told defendant that they were looking for drugs and drug-related items rather than computer files containing child pornography) (citing *Turner*). Of course, as with other scope-of-consent cases, cases analyzing the reason for a search are fact specific, and courts' interpretations of the scope of consent are not always narrow. *See United States v. Marshall*, 348 F.3d 281, 287-88 (1st Cir. 2003) (finding that consent to search for "stolen items" did not preclude seizing and viewing video tapes where video equipment, but not video tapes, were reported stolen); *United States v. Raney*, 342 F.3d 551, 556-58 (7th Cir. 2003) (finding consent to search for "materials in the nature of" child exploitation and child erotica was broad enough to encompass search of homemade adult pornography where the defendant had expressed an intent to make similar homemade pornography with a minor).

Finally, the scope of consent usually relates to the target item, location, and purpose of the search, rather than the search methodology used. For example, in *United States v. Brooks*, 427 F.3d 1246 (10th Cir. 2005), an agent received permission to conduct a "complete search" of the defendant's computer for child pornography. The agent explained that he would use a "pre-search" disk to find and display image files, allowing the agent to easily ascertain whether any images contained child pornography. *Id.* at 1248. When the disk, for unexplained reasons, failed to function, the agent conducted a manual search for image files, eventually discovering several pieces of child pornography. *Id*. Although the agent ultimately used a different search methodology than the one he described to the defendant, the Court approved the manual search because it did not exceed the scope of the described disk search. *Id*. at 1249-50. *See also United States v. Long*, 425 F.3d 482, 487 (7th Cir. 2005) (finding that agent's use of "sophisticated" Encase forensic software did not exceed scope of consent to search laptop).

☞ It is a good practice for agents to use written consent forms that state explicitly that the scope of consent includes consent to search computers and other electronic storage devices.

Because the decisions evaluating the scope of consent to search computers have reached sometimes unpredictable results, investigators should indicate the scope of the search explicitly when obtaining a suspect's consent to search a computer. Moreover, investigators who have seized a computer based on consent and who have developed probable cause may consider obviating concerns with either the scope of consent or revocation of consent by obtaining a search warrant. For a sample consent to search form, see Appendix J.

b. Third-Party Consent

i. General Principles

It is common for several people to use or own the same computer equipment. If any one of those people gives permission to search for data, agents may generally rely on that consent, so long as the person has authority over the computer. In such cases, all users have assumed the risk that a co-user might discover everything in the computer and might also permit law enforcement to search this "common area" as well.

The watershed case in this area is *United States v. Matlock*, 415 U.S. 164 (1974). In *Matlock*, the Supreme Court stated that one who has "common

authority" over premises or effects may consent to a search even if an absent co-user objects. *Id.* at 171. According to the Court, the common authority that establishes the right of third-party consent requires

> mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Id. at 171 n.7.

Under the *Matlock* approach, a private third party may consent to a search of property under the third party's joint access or control. Agents may view what the third party may see without violating any reasonable expectation of privacy so long as they limit the search to the zone of the consenting third party's common authority. *See United States v. Jacobsen*, 466 U.S. 109, 119-20 (1984) (noting that the Fourth Amendment is not violated when a private third party invites the government to view the contents of a package under the third party's control). This rule often requires agents to inquire into third parties' rights of access before conducting a consent search and to draw lines between those areas that fall within the third party's common authority and those areas outside of the third party's control. *See United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978) (holding that a mother could consent to a general search of her 23-year-old son's room, but could not consent to a search of a locked footlocker found in the room).

Co-users of a computer will generally have the ability to consent to a search of its files under *Matlock*. *See United States v. Smith*, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (concluding that a woman could consent to a search of her boyfriend's computer located in their house and noting that the boyfriend had not password-protected his files). However, when an individual protects her files with passwords and has not shared the passwords with others who also use the computer, the Fourth Circuit has held that the authority of those other users to consent to search of the computer will not extend to the password-protected files. *See Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (analogizing password-protected files to locked footlockers inside a bedroom, which the court had previously held to be outside the scope of common authority consent). Nevertheless, specific facts may overcome an

individual's expectation of privacy even in password-protected files. In *United States v. Buckner*, 407 F. Supp. 2d 777 (W.D. Va. 2006), the Court held that the defendant's wife could validly consent to a search of the family computer, including her husband's password-protected files. The Court distinguished *Trulock* by noting that the computer was leased solely in the wife's name, the allegedly fraudulent activity that provoked the search had occurred through accounts in the wife's name, the computer was located in a common area of the house, none of the files were encrypted, and the computer was on even though the husband had apparently fled the area. *Id.* at 780-81. Furthermore, if the co-user has been given the password by the suspect, then she probably has the requisite common authority to consent to a search of the files under *Matlock*. *See United States v. Murphy*, 506 F.2d 529, 530 (9th Cir. 1974) (per curiam) (concluding that an employee could consent to a search of an employer's locked warehouse because the employee possessed the key, and finding "special significance" in the fact that the employer had himself delivered the key to the employee).

As a practical matter, agents may have little way of knowing the precise bounds of a third party's common authority when the agents obtain third-party consent to conduct a search. When queried, consenting third parties may falsely claim that they have common authority over property. In *Illinois v. Rodriguez*, 497 U.S. 177 (1990), the Supreme Court held that the Fourth Amendment does not automatically require suppression of evidence discovered during a consent search when it later comes to light that the third party who consented to the search lacked the authority to do so. *See id.* at 188-89. Instead, the Court held that agents can rely on a claim of authority to consent if based on "the facts available to the officer at the moment, . . . a man of reasonable caution . . . [would believe] that the consenting party had authority" to consent to a search of the premises. *Id.* (internal quotation marks omitted) (quoting *Terry v. Ohio*, 392 U.S. 1, 21-22 (1968)). When agents reasonably rely on apparent authority to consent, the resulting search does not violate the Fourth Amendment. For example, in *United States v. Morgan*, 435 F.3d 660 (6th Cir. 2006), investigators received consent from the defendant's wife to search a computer located in the common area of the home. The wife told police that she had access to the computer, that neither she nor her husband used individual usernames or passwords, and that she had recently installed spyware on the computer to monitor her husband's suspected viewing of child pornography. *Id.* at 663-64. She did not tell the police that she had her own, separate computer for her primary use. *Id.* at 662. Nevertheless, the Court

found that the police could reasonably rely on her statements and conclude that she had authority to consent to the search. *Id.* at 664. *See also United States v. Andrus*, 483 F.3d 711, 720-21 (10th Cir. 2007) (holding that parent had apparent authority to consent to search of computer in room of adult child, where parent had unrestricted access to adult child's bedroom and paid for Internet access).

The Supreme Court has held, however, that investigators cannot rely on a third party's consent to search a residence when the target of the search is present and expressly objects to the search. *See Georgia v. Randolph*, 547 U.S. 103, 121 (2006). The court's conclusion was based on its determination that a "co-tenant wishing to open the door to a third party has no recognized authority in law or social practice to prevail over a present and objecting co-tenant." *Id.* at 114. Moreover, unless police remove a potential objector "for the sake of avoiding a possible objection," *Randolph* does not apply to "potential" objectors who have not taken part in the consent colloquy, even if the potential objector is nearby. *Id*. at 121. For example, in *United States v. Hudspeth*, 518 F.3d 954 (8th Cir. 2008) (en banc), officers arrested the defendant at his workplace for possession of child pornography, and the defendant refused to consent to a search of his home. Nevertheless, his wife subsequently consented to a search of a computer in their home. The Eighth Circuit upheld the search, explaining that "unlike *Randolph*, the officers in the present case were not confronted with a 'social custom' dilemma, where two physically present co-tenants have contemporaneous competing interests and one consents to a search, while the other objects." *Id.* at 960. *See also United States v. Crosbie*, 2006 WL 1663667, at *2 (S.D. Ala. June 9, 2006) (defendant's wife's consent to computer search was valid even though wife had ordered her husband out of the house, thus depriving him of the "opportunity to object").

ii. Spouses and Domestic Partners

☞ Most spousal consent searches are valid.

Absent an affirmative showing that the consenting spouse has no access to the property searched, the courts generally hold that either spouse may consent to a search of all of the couple's property. *See, e.g.*, *Trulock v. Freeh*, 275 F.3d 391, 398, 403-04 (4th Cir. 2001) (holding that woman did not have authority to consent to search of computer files of the man with whom she lived, when she had told agents that she did not know the password to access his files); *United States v. Duran*, 957 F.2d 499, 504-05 (7th Cir. 1992) (concluding that

wife could consent to search of barn she did not use because husband had not denied her the right to enter barn); *United States v. Long*, 524 F.2d 660, 661 (9th Cir. 1975) (holding that wife who had left her husband could consent to search of jointly-owned home even though husband had changed the locks). For example, in *United States v. Smith*, 27 F. Supp. 2d 1111 (C.D. Ill. 1998), a man named Smith was living with a woman named Ushman and her two daughters. When allegations of child molestation were raised against Smith, Ushman consented to the search of his computer, which was located in the house in an alcove connected to the master bedroom. Although Ushman used Smith's computer only rarely, the district court held that she could consent to the search of Smith's computer. Because Ushman was not prohibited from entering the alcove and Smith had not password-protected the computer, the court reasoned, she had authority to consent to the search. *See id.* at 1115-16. Even if she lacked actual authority to consent, the court added, she had apparent authority to consent. *See id.* at 1116 (citing *Illinois v. Rodriguez*, 497 U.S. 177 (1990)).

iii. Parents

☞ Parents can consent to searches of their children's computers when the children are under 18 years old. If the children are 18 or older, the parents may or may not be able to consent, depending on the facts.

In some computer crime cases, the perpetrators are relatively young and reside with their parents. When the perpetrator is a minor, parental consent to search the perpetrator's property and living space will almost always be valid. *See* 3 Wayne LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 8.4(b) at 283 (2d ed. 1987) (noting that courts have rejected "even rather extraordinary efforts by [minor] child[ren] to establish exclusive use.").

When the sons and daughters who reside with their parents are legal adults, however, the issue is more complicated. Under *Matlock*, it is clear that parents may consent to a search of common areas in the family home regardless of the perpetrator's age. *See, e.g.*, *United States v. Lavin*, 1992 WL 373486, at *6 (S.D.N.Y. Nov. 30, 1992) (recognizing right of parents to consent to search of basement room where son kept his computer and files). When agents would like to search an adult child's room or other private areas, however, agents cannot assume that the adult's parents have authority to consent. Although courts have offered divergent approaches, they have paid particular attention

to three factors: the suspect's age; whether the suspect pays rent; and whether the suspect has taken affirmative steps to deny his or her parents access to the suspect's room or private area. When suspects are older, pay rent, and/or deny access to parents, courts have generally held that parents may not consent. *See United States v. Whitfield*, 939 F.2d 1071, 1075 (D.C. Cir. 1991) ("cursory questioning" of suspect's mother insufficient to establish right to consent to search of 29-year-old son's room); *United States v. Durham*, 1998 WL 684241, at *4 (D. Kan. Sept. 11, 1998) (mother had neither apparent nor actual authority to consent to search of 24-year-old son's room, because son had changed the locks to the room without telling his mother, and son also paid rent for the room). In contrast, parents usually may consent if their adult children do not pay rent, are fairly young, and have taken no steps to deny their parents access to the space to be searched. *See United States v. Andrus*, 483 F.3d 711, 713, 720-21 (10th Cir. 2007) (parent had apparent authority to consent to search of computer in room of 51-year-old son who did not pay rent, where parent had unrestricted access to adult child's bedroom and paid for Internet access); *United States v. Rith*, 164 F.3d 1323, 1331 (10th Cir. 1999) (suggesting that parents were presumed to have authority to consent to a search of their 18-year-old son's room because he did not pay rent); *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978) (mother could consent to police search of 23-year-old son's room when son did not pay rent).

iv. Computer Repair Technicians

As discussed above in Section B.4, computer searches by repairman prior to contact with law enforcement are private searches and do not implicate the Fourth Amendment. Most commonly, law enforcement will use information revealed through a repairman's private search as a basis to secure a warrant for a full search of the computer. In some cases, however, law enforcement officers have relied on the consent of the repairman as the basis for a search of the computer that exceeds the scope of the initial private search. District courts have split on whether computer repairmen have the authority to authorize such searches. *Compare United States v. Anderson*, 2007 WL 1121319, at *6 (N.D. Ind. Apr. 16, 2007) (technicians had "actual and apparent authority" to consent to a search of computer brought in for repair because they had authority to access the computer), *with United States v. Barth*, 26 F. Supp. 2d 929, 938 (W.D. Tex. 1998) (repairman lacked actual or apparent authority to consent to search of hard drive because the defendant had given the hard drive

to the technician only for a limited purpose unrelated to the specific files and only for a limited period of time).

v. System Administrators

Computer network accounts, including the accounts provided by private employers to their employees, by government entities to public employees, and by large commercial service providers to their customers, often contain information relevant to criminal investigations. When investigators suspect that a computer network account contains relevant evidence, they may want to know whether the network's owner or manager has authority to voluntarily disclose information related to the account. As a practical matter, every computer network is managed by a "system administrator" or "system operator" whose job is to keep the network running smoothly, monitor security, and repair the network when problems arise. System operators have "root level" access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems. However, whether a system administrator (generally at the direction of an appropriate supervisory official) may voluntarily consent to disclose information from or regarding a user's account varies based on whether the network belongs to a communication service provider, a private business, or a government entity.

Regarding public commercial communication service providers (such as Google or Yahoo!), the primary barrier to voluntary disclosure by the service provider is statutory, not constitutional. As discussed in Chapter 3, any attempt to obtain a system administrator's consent to disclose information regarding an account must comply with the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712. Section 2702 of the SCA prohibits public service providers from voluntarily disclosing to the government information pertaining to their customers except in certain specified situations—which often track Fourth Amendment exceptions—such as with the consent of the user, to protect the service provider's rights and property, or in an emergency. *See* Chapter 3.E, *infra*. Significantly for Fourth Amendment purposes, commercial service providers typically have terms of service that confirm their authority to access information stored on their systems, and such terms of service may establish a service provider's common authority over their users' accounts. *See United States v. Young*, 350 F.3d 1302, 1308-09 (11th Cir. 2003) (holding that Federal Express's terms of service, which authorized it to inspect packages, gave it common authority to consent to a government search of a package); *see also United States v. Beckett*, 544 F. Supp. 2d 1346, 1350 (S.D. Fla. 2008) ("where

service providers have an agreement to share information under circumstances similar to those in our case (for investigation, to cooperate with law enforcement, and to take legal action), there is no objectively reasonable expectation of privacy and therefore no Fourth Amendment protection for subscriber information"). *But see Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-08 (9th Cir. 2008) (finding government employee had reasonable expectation of privacy in pager messages stored by provider of communication service based on "informal policy that the text messages would not be audited").

As discussed more fully in Section D.1.b below, private-sector employers generally have broad authority to consent to searches in the workplace, and this authority extends to workplace networks. For example, in *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), the Ninth Circuit held that an employer could consent to a search of the computer it provided to an employee and stated that "the computer is the type of workplace property that remains within the control of the employer even if the employee has placed personal items in it." *Id.* at 1191 (internal quotation marks omitted). Thus, law enforcement can generally rely on the consent of an appropriate manager to search a private workplace network. In contrast, as discussed in Section D.2 below, the Fourth Amendment rules for government computer networks differ significantly from the rules that apply to private networks. Searches of government computer networks are *not* evaluated under *Matlock*; instead, they are evaluated under the standards of *O'Connor v. Ortega*, 480 U.S. 709 (1987).

c. Implied Consent

Individuals often enter into agreements with the government in which they waive some of their Fourth Amendment rights. For example, prison guards may agree to be searched for drugs as a condition of employment, and visitors to government buildings may agree to a limited search of their person and property as a condition of entrance. Similarly, users of computer systems may waive their rights to privacy as a condition of using the systems. When individuals who have waived their rights are then searched and challenge the searches on Fourth Amendment grounds, courts typically focus on whether the waiver eliminated the individual's reasonable expectation of privacy against the search. *See, e.g.*, *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (government employee had no reasonable expectation of privacy in computer in light of computer use policy); *American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Service*, 871 F.2d 556, 559-61 (6th Cir. 1989) (postal employees retained no reasonable expectation of privacy

in government lockers after signing waivers). For an expanded discussion of workplace searches, *see* Section D below.

A few courts have approached the same problem from a slightly different direction and have asked whether the waiver established implied consent to the search. According to the doctrine of implied consent, consent to a search may be inferred from an individual's conduct. For example, in *United States v. Ellis*, 547 F.2d 863 (5th Cir. 1977), a civilian visiting a naval air station agreed to post a visitor's pass on the windshield of his car as a condition of bringing the car on the base. The pass stated that "[a]cceptance of this pass gives your consent to search this vehicle while entering, aboard, or leaving this station." *Id.* at 865 n.1. During the visitor's stay on the base, a station investigator who suspected that the visitor had stored marijuana in the car approached the visitor and asked him if he had read the pass. After the visitor admitted that he had, the investigator searched the car and found 20 plastic bags containing marijuana. The Fifth Circuit ruled that the warrantless search of the car was permissible, because the visitor had impliedly consented to the search when he knowingly and voluntarily entered the base with full knowledge of the terms of the visitor's pass. *See id.* at 866-67.

Ellis notwithstanding, it must be noted that several circuits have been critical of the implied consent doctrine in the Fourth Amendment context. Despite the Fifth Circuit's broad construction, other courts have been reluctant to apply the doctrine absent evidence that the suspect actually knew of the search and voluntarily consented to it at the time the search occurred. *See McGann v. Northeast Illinois Regional Commuter R.R. Corp.*, 8 F.3d 1174, 1180 (7th Cir. 1993) ("Courts confronted with claims of implied consent have been reluctant to uphold a warrantless search based simply on actions taken in the light of a posted notice."); *Security and Law Enforcement Employees, Dist. Council 82 v. Carey*, 737 F.2d 187, 202 n.23 (2d Cir. 1984) (rejecting argument that prison guards impliedly consented to search by accepting employment at prison where consent to search was a condition of employment). Absent such evidence, these courts have preferred to examine general waivers of Fourth Amendment rights solely under the reasonable-expectation-of-privacy test. *See id.*

2. Exigent Circumstances

The exigent circumstances exception to the warrant requirement generally applies when one of the following circumstances is present: (1) evidence is in imminent danger of destruction; (2) a threat puts either the police or the

public in danger; (3) the police are in "hot pursuit" of a suspect; or (4) the suspect is likely to flee before the officer can secure a search warrant. *Georgia v. Randolph*, 547 U.S. 103, 117 n.6 (2006) (collecting cases); *Brigham City v. Stuart*, 547 U.S. 398, 403-06 (2006) (police appropriately entered house to stop assault when occupants did not respond to the officers' verbal directions); *Illinois v. McArthur*, 531 U.S. 326, 331-33 (2001) (police appropriately seized house for two hours while warrant was obtained); *Cupp v. Murphy*, 412 U.S. 291, 294-96 (1973) (murder suspect was temporarily seized and his fingernails scraped to prevent destruction of evidence). Of the four factors justifying an exigent circumstances search, the first—that the evidence is in imminent danger of destruction—is generally the most relevant in the context of computer searches.

In determining whether exigent circumstances exist, agents should consider: (1) the degree of urgency involved, (2) the amount of time necessary to obtain a warrant, (3) whether the evidence is about to be removed or destroyed, (4) the possibility of danger at the site, (5) whether those in possession of the contraband know that the police are on their trail, and (6) the ready destructibility of the contraband. *See United States v. Reed,* 935 F.2d 641, 642 (4th Cir. 1991); *see also United States v. Plavcak*, 411 F.3d 655, 664-65 (6th Cir. 2005) (agents appropriately seized computer without warrant when targets were caught burning relevant documentary evidence and then ran from residence carrying computer); *United States v. Trowbridge*, 2007 WL 4226385, at *4-5 (N.D. Tex. Nov. 29, 2007) (agents appropriately seized computers without a warrant based on exigent circumstances where agents were concerned for their safety during a fast-moving investigation and it was likely that computer evidence would be destroyed).

Exigent circumstances can arise in computer cases before the evidence has been properly secured because electronic data is inherently perishable. Computer data can be effectively put out of law enforcement reach with widely-available and powerful encryption programs that can be triggered with just a few keystrokes. In addition, computer commands can destroy data in a matter of seconds, as can moisture, high temperature, physical mutilation, or magnetic fields created, for example, by passing a strong magnet over a disk. For example, in *United States v. David*, 756 F. Supp. 1385 (D. Nev. 1991), agents saw the defendant deleting files on his computer and seized the computer immediately. The district court held that the agents did not need a warrant to seize the computer because the defendant's acts had created exigent circumstances. *See*

id. at 1392. *See also United States v. Gorshkov*, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001) (circumstances justified downloading without a warrant data from computer in Russia where probable cause existed to believe that Russian computer contained evidence of crime, where good reason existed to fear that delay could lead to destruction of or loss of access to evidence, and where agent merely copied data and subsequently obtained search warrant).

With some electronic devices, exigent circumstances may arise because information may be lost when the device's battery dies, or new information may cause older information to be lost permanently. For example, in *United States v. Romero-Garcia*, 991 F. Supp. 1223, 1225 (D. Or. 1997), *aff'd on other grounds* 168 F.3d 502 (9th Cir. 1999), a district court held that agents had properly accessed the information in an electronic pager in their possession because they had reasonably believed that it was necessary to prevent the destruction of evidence. The information stored in pagers is readily destroyed, the court noted: incoming messages can delete stored information, or the batteries can die, erasing the information. Accordingly, the agents were justified in accessing the pager without first acquiring a warrant. *See also United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (in conducting search incident to arrest, agents were justified in retrieving numbers from pager because pager information is easily destroyed). In *United States v. Parada*, 289 F. Supp. 2d 1291 (D. Kan. 2003), a court reached the same result for a cell phone, although the court's analysis may have been based in part on a misunderstanding of how cell phones function. The court held that exigent circumstances justified the search of a cell phone because the phone had limited memory and subsequent calls could overwrite previously stored numbers, whether the phone was on or off. *See id.* at 1303-04.

However, in electronic device cases, as in all others, the existence of exigent circumstances is tied to the facts of the individual case, and other courts have rejected claims that exigent circumstances justified a search of an electronic device. For example, in *United States v. Morales-Ortiz*, 376 F. Supp. 2d 1131, 1142 (D.N.M. 2004), the court held that exigent circumstances did not justify a search of the names and numbers held within a cell phone's address book. The court distinguished a search of the cell phone's address book records from the search of the incoming call log approved in *Parada*. *See id.*; s*ee also United States v. Wall*, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008) (noting that cell phones store text messages until they are deleted by the user and therefore rejecting argument that exigent circumstances justified search of seized cell

phone); *David*, 756 F. Supp at 1392 n.2 (dismissing as lame the government's argument that exigent circumstances supported search of a battery-operated computer because the agent did not know how much longer the computer's batteries would live); *United States v. Reyes*, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996) (exigent circumstances could not justify search of a pager because the government agent unlawfully created the exigency by turning on the pager).

Recent technological advances in pagers, cell phones, and PDAs may have an impact on the existence of exigent circumstances justifying the search of these devices without a warrant. Some of the advances may undercut the basis for finding exigent circumstances. For example, current electronic devices are more likely to rely on a storage mechanism (such as flash memory) that does not require battery power to maintain storage. However, other technological advances have created new exigencies. For example, a "kill command" can be sent to some devices that will cause the device to encrypt itself or overwrite data stored on the device. Similarly, other devices can be set to delete information stored on the device after a certain period of time. *See United States v. Young*, 2006 WL 1302667, at *13 (N.D.W.Va. May 9, 2006) (exigent circumstances justified searching a cell phone for text messages where the cell phone had an option for automatically deleting text messages after one day).

Importantly, because "a warrantless search must be strictly circumscribed by the exigencies which justify its initiation," *Mincey v. Arizona*, 437 U.S. 385, 393 (1978) (internal quotation marks omitted), exigent circumstances that support the warrantless seizure of a computer may not support the subsequent search of the computer by law enforcement. "Recognizing the generally less intrusive nature of a seizure, the [Supreme] Court has frequently approved warrantless seizures of property, on the basis of probable cause, for the time necessary to secure a warrant." *Segura v. United States*, 468 U.S. 796, 806 (1984) (internal citations omitted). Thus, the need to seize a container to prevent the destruction of evidence does not necessarily authorize agents to take further steps without a warrant. *See United States v. Doe*, 61 F.3d 107, 110-11 (1st Cir. 1995); *David*, 756 F. Supp. at 1392 (exigency justified seizure but not search of computer); *Morales-Ortiz*, 376 F. Supp. 2d at 1142 n.2 (emphasizing that while exigent circumstances may justify seizing a pager to preserve evidence, the exception does not justify manipulating the pager in order to retrieve messages). In addition, absent an immediate need to access the data, practical factors may favor a forensic analysis of a seized computer based on a search warrant. A trained analyst working in a forensic setting can often

extract detailed and relevant information from a computer that would not be recovered through a hastily conducted search.

3. Search Incident to a Lawful Arrest

Pursuant to a lawful arrest, agents may conduct a "full search" of the arrested person, and a more limited search of his surrounding area, without a warrant. *See United States v. Robinson*, 414 U.S. 218, 235 (1973); *Chimel v. California*, 395 U.S. 752, 762-63 (1969). For example, in *Robinson*, a police officer conducting a patdown search incident to an arrest for a traffic offense discovered a crumpled cigarette package in the suspect's left breast pocket. Not knowing what the package contained, the officer opened the package and discovered fourteen capsules of heroin. The Supreme Court held that the search of the package was permissible, even though the officer had no articulable reason to open the package. *See Robinson*, 414 U.S. at 234-35. In light of the general need to preserve evidence and prevent harm to the arresting officer, the Court reasoned, it was *per se* reasonable for an officer to conduct a "full search of the person" pursuant to a lawful arrest. *Id.* at 235.

The permissible temporal scope for a search incident to arrest varies based on whether the item searched is an item "immediately associated with the person of an arrestee," such as clothing or a wallet, or other personal property near the arrestee, such as luggage. *United States v. Chadwick*, 433 U.S. 1, 15 (1977). Two Supreme Court cases illustrate this distinction. First, *United States v. Edwards*, 415 U.S. 800, 808-09 (1974), demonstrates the substantial time allowed for a search incident to arrest of items immediately associated with the person of an arrestee: the Court upheld a search of a defendant's clothing after a night in jail. In contrast, in *United States v. Chadwick*, the Court held that officers impermissibly searched a footlocker seized incident to arrest when they searched the locker away from the site of the arrest ninety minutes after the arrest. *See Chadwick*, 433 U.S. at 14-16. The Court stated that "[o]nce law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest." *Id.* at 15.

The Supreme Court recently revisited the search incident to arrest doctrine in *Arizona v. Gant*, 129 S. Ct. 1710 (2009). There, the Court authorized a search of a passenger compartment of a vehicle incident to arrest in only two

situations: first, "when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search"; and second, "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle." *Id.* at 1719 (internal quotation marks omitted). Caution is appropriate until courts consider whether the reasoning of *Gant* is limited to vehicle searches, but there is good reason to conclude that the "evidence relevant to the crime of arrest" requirement should apply only to such searches. *Gant* states that its second exception is based on "circumstances unique to the vehicle context" and cites Justice Scalia's concurrence in *Thornton v. United States*, 541 U.S. 615, 632 (2004). That concurrence proposed the second exception in the context of vehicle searches and explained that "[a] motorist may be arrested for a wide variety of offenses; in many cases, there is no reasonable basis to believe relevant evidence might be found in the car." *Thornton*, 541 U.S. at 632.

Beginning with pagers and now extending to cell phones and personal digital assistants, courts have generally agreed that the search incident to arrest doctrine applies to portable electronic devices. First, numerous cases over the last decade have approved searches of pagers incident to arrest. *See United States v. Brookes*, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005); *Yu v. United States*, 1997 WL 423070, at *2 (S.D.N.Y. Jul. 29, 1997); *United States v. Thomas*, 114 F.3d 403, 404 n.2 (3d Cir. 1997) (dicta); *United States v. Reyes*, 922 F. Supp. 818, 833 (S.D.N.Y. 1996); *United States v. Lynch*, 908 F. Supp. 284, 287 (D.V.I. 1995); *United States v. Chan*, 830 F. Supp. 531, 535 (N.D. Cal. 1993); *see also United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (same holding, but relying on an exigency theory). More recently, many courts have upheld searches of cell phones incident to arrest. *United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007); *United States v. Valdez*, 2008 WL 360548, at *2-4 (E.D. Wis. Feb. 8, 2008); *United States v. Curry*, 2008 WL 219966, at *10 (D. Me. Jan. 23, 2008); *United States v. Mercado-Nava*, 486 F. Supp. 2d 1271, 1278-79 (D. Kan. 2007); *United States v. Dennis*, 2007 WL 3400500, at *7-8 (E.D. Ky. Nov. 13, 2007); *United States v. Mendoza*, 421 F.3d 663, 666-68 (8th Cir. 2005); *United States v. Brookes*, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005); *United States v. Cote*, 2005 WL 1323343, at *6 (N.D. Ill. May 26, 2005). In addition, one appellate court has approved a search incident to arrest of an electronic address book. *See United States v. Goree*, 2002 WL 31050979, at *5-6 (6th Cir. Sept. 12, 2002).

Courts have disagreed about whether a search incident to arrest of a cell phone is more like the footlocker in *Chadwick* (and thus subject to strict

temporal requirements) or the search of the personal property in *Edwards* (and thus subject to more flexible temporal requirements). The only appellate court to consider the issue held that a cell phone found on the defendant's person constitutes personal property "immediately associated" with the arrestee. *Finley*, 477 F.3d at 260 n.7. *See also United States v. Wurie*, 2009 WL 1176946, at *5 (D. Mass. 2009); *Brookes*, 2005 WL 1940124, at *3 (analogizing pager and cell phone to wallet or address book); *Cote*, 2005 WL 1323343, at *6 (upholding search of cell phone at police station two and a half hours after arrest). However, two district courts have analogized cell phones to the footlocker in *Chadwick* and held that cell phone searches not contemporaneous with arrest violated the Fourth Amendment. *See United States v. Lasalle*, 2007 WL 1390820, at *7 (D. Haw. May 9, 2007) (rejecting cell phone search more than two hours and fifteen minutes after arrest); *United States v. Park*, 2007 WL 1521573, at *5-9 (N.D. Cal. May 23, 2007) (rejecting cell phone search approximately ninety minutes after arrest). S*ee also United States v. Wall*, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008) (search of cell phone performed at stationhouse after arrest could not be justified as incident to arrest).

Courts have not yet addressed whether electronic media with the vast storage capacity of today's laptop computers may be searched incident to arrest. However, courts have allowed extensive searches of written materials discovered incident to lawful arrests. For example, courts have uniformly held that agents may inspect the entire contents of a suspect's wallet found on his person. *See, e.g.*, *United States v. Molinaro*, 877 F.2d 1341, 1347 (7th Cir. 1989) (citing cases); *United States v. Castro*, 596 F.2d 674, 677 (5th Cir. 1979). Similarly, one court has held that agents could photocopy the entire contents of an address book found on the defendant's person during the arrest, *see United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993), and others have permitted the search of a defendant's briefcase that was at his side at the time of arrest. *See, e.g.*, *United States v. Johnson*, 846 F.2d 279, 283-84 (5th Cir. 1988); *United States v. Lam Muk Chiu*, 522 F.2d 330, 332 (2d Cir. 1975). If these holdings are applied to searches incident to arrest where computers and similar storage media are recovered, agents should be able to review the contents of such devices without securing a search warrant.

On the other hand, courts may analogize a laptop to the footlocker in *Chadwick*, so a search incident to arrest of a laptop may be judged under *Chadwick*'s restrictive temporal standard if it is not seized from the suspect's person. As a practical matter, it may not be feasible to conduct an appropriate

search of a laptop incident to arrest (though a brief review may be possible in some cases, particularly as forensic tools designed for on-site review become available). A complete forensic search often requires that the data on a computer be copied and then searched using tools designed for forensic analysis, and such a full search may be impossible under *Chadwick*. Instead, agents may choose to seize a laptop incident to arrest and then obtain a search warrant for the subsequent thorough search.[6] When making an arrest, seizure of items on the arrestee's person or within his reach is entirely appropriate. *See Edwards*, 415 U.S. at 805.

4. Plain View

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. To rely on this exception, the agent must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent. *See Horton v. California*, 496 U.S. 128, 136 (1990). Although officers may occasionally come upon incriminating evidence on the screen of a computer, the most common use of the plain view doctrine in the computer context occurs when agents examine a computer pursuant to a search warrant and discover evidence of a separate crime that falls outside the scope of the search warrant. For example, in *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003), an agent discovered child pornography on a hard drive while conducting a valid search of the drive for evidence of a murder. Because the agent was properly searching graphics files for evidence of the murder, the child pornography was properly seized and subsequently admitted under the plain view doctrine. The plain view doctrine can also be useful in other circumstances when agents are lawfully in a position to discover incriminating evidence on a computer. *See, e.g.*, *United States v. Herndon*, 501 F.3d 683, 693 (6th Cir. 2007) (officer permissibly seized a computer based upon plain view after a probation agent showed the officer child pornography discovered on subject's computer); *United States v. Tucker*, 305 F.3d 1193, 1203 (10th Cir. 2002) (approving seizure of computer under plain view doctrine by officer conducting parole search of home after officer noticed that computer had recently visited child pornography newsgroup). Most computer

[6] In addition, cell phones increasingly resemble computers, as they now may incorporate functions such as Internet, email, and photography. A complete forensic search of such cell phones may disclose more evidence than a brief search incident to arrest. *See generally* Wayne Jansen and Rick Ayers, *Guidelines on Cell Phone Forensics* (National Institute of Standards and Technology No. 800-101, 2007).

plain view cases involve agents viewing incriminating images, but in some circumstances the names associated with files (especially child pornography) can be incriminating as well. *Compare Commonwealth v. Hinds*, 768 N.E.2d 1067, 1073 (Mass. 2002) (finding that an officer lawfully searching for evidence of assault could open and seize image files whose sexually explicit names were in "plain view" and incriminating), *with United States v. Stierhoff*, 477 F. Supp. 2d 423, 445-49 (D.R.I. 2007) (rejecting the government's argument that the label on a computer file, "offshore," was sufficiently incriminating to justify opening the file under the plain view exception).

☞ The plain view doctrine does not authorize agents to open and view the contents of a container that they are not otherwise authorized to open and review.

Importantly, the plain view exception cannot justify violations of an individual's reasonable expectation of privacy. The exception merely permits the seizure of evidence that an agent is already authorized to view in accordance with the Fourth Amendment. This means that agents cannot rely on the plain view exception to justify opening a closed container that they are not otherwise authorized to view. *See United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996) (holding that computer files opened by agents were not in plain view); *United States v. Villarreal*, 963 F.2d 770, 776 (5th Cir. 1992) (concluding that labels fixed to opaque 55-gallon drums do not expose the contents of the drums to plain view because "a label on a container is not an invitation to search it"). As discussed above in Section B.2, courts have reached differing conclusions over whether each individual file stored on a computer should be treated as a separate closed container, and this distinction has important ramifications for the scope of the plain view exception. Most courts have analyzed individual computer files as separate stored containers. *See Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001); *United States v. Carey*, 172 F.3d 1268, 1273-75 (10th Cir. 1999). When each file is treated as a separate closed container, agents cannot rely on the plain view doctrine to open files on a computer. However, Fifth Circuit decisions in *United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001), and *United States v. Slanina*, 283 F.3d 670, 680 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *aff'd*, 359 F.3d 356, 358 (5th Cir. 2004), suggest that plain view of a single file on a computer or storage device could provide a basis for a more extensive search. In those two cases, the court held that when a warrantless search of a portion of a computer or storage device had been proper, the defendant no longer retained any reasonable expectation

of privacy in the remaining contents of the computer or storage device. *See Slanina*, 283 F.3d at 680; *Runyan*, 275 F.3d at 464-65. Thus, a more extensive search of the computer or storage device by law enforcement did not violate the Fourth Amendment. This rationale may also apply when a file has been placed in plain view.

The plain view doctrine arises frequently in the search warrant context because it is usually necessary to review all files on a computer to find evidence that falls within the scope of a warrant. As the Ninth Circuit explained in *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006), "[c]omputer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol [*e.g.*, key word searches], much evidence could escape discovery simply because of [the defendants'] labeling of the files." As agents review a computer for information that falls within the scope of the warrant, they may discover evidence of an additional crime, and they are entitled to seize it under the plain view doctrine. Nevertheless, the Tenth Circuit's decision in *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999), provides a cautionary example regarding continuing the review of a computer after finding evidence of a second crime. In *Carey*, a police detective searching a hard drive with a warrant for drug trafficking evidence opened a "jpg" file and instead discovered child pornography. At that point, the detective spent five hours accessing and downloading several hundred "jpg" files in a search not for evidence of the narcotics trafficking that he was authorized to seek and gather pursuant to the original warrant, but for more child pornography. When the defendant moved to exclude the child pornography files on the ground that they were seized beyond the scope of the warrant, the government argued that the detective had seized the "jpg" files properly because the contents of the contraband files were in plain view. The Tenth Circuit rejected this argument with respect to all of the files except for the first "jpg" file the detective discovered. *See id.* at 1273, 1273 n.4. As best as can be discerned, the rule in *Carey* seems to be that the detective could seize the first "jpg" file that came into plain view when the detective was executing the search warrant, but could not rely on the plain view exception to justify the search solely for additional "jpg" files containing child pornography on the defendant's computers, evidence beyond the scope of the warrant. In subsequent cases, the Tenth Circuit has interpreted *Carey* narrowly, explaining that it "simply stands for the proposition that law enforcement may not expand the scope of a search beyond its original justification." *United States v. Grimmett,* 439 F.3d 1263, 1268 (10th Cir. 2006). For example, in *United States v. Walser*, 275 F.3d 981, 986-87 (10th Cir. 2001), the court found no

Fourth Amendment violation when an officer with a warrant to search for electronic records of drug transactions opened a single computer file containing child pornography, suspended the search, and then returned to a magistrate for a second warrant to search for child pornography. *See also United States v. Kearns*, 2006 WL 2668544, at *8 (N.D. Ga. Feb. 21, 2006) (suggesting that agent who opened every file on a compact disk, regardless of file extension, in a search for evidence of fraud could have seized images of child pornography under the "plain view" doctrine as long as he did not abandon his search).

5. Inventory Searches

Law enforcement officers routinely inventory the items they have seized. Such "inventory searches" are reasonable—and therefore fall under an exception to the warrant requirement—when two conditions are met. First, the search must serve a legitimate, non-investigatory purpose (*e.g.*, to protect an owner's property while in custody; to insure against claims of lost, stolen, or vandalized property; or to guard the police from danger) that outweighs the intrusion on the individual's Fourth Amendment rights. *See Illinois v. Lafayette,* 462 U.S. 640, 644 (1983); *South Dakota v. Opperman*, 428 U.S. 364, 369-70 (1976). Second, the search must follow standardized procedures. *See Colorado v. Bertine*, 479 U.S. 367, 374 n.6 (1987); *Florida v. Wells*, 495 U.S. 1, 4-5 (1990).

It is unlikely that the inventory-search exception to the warrant requirement would support a search of seized computer files. *See United States v. O'Razvi*, 1998 WL 405048, at *6-7 (S.D.N.Y. July 17, 1998) (noting the difficulties of applying the inventory-search requirements to computer disks); *see also United States v. Wall*, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) (inventory search exception did not justify search of cell phone); *United States v. Flores*, 122 F. Supp. 2d 491, 493-95 (S.D.N.Y. 2000) (finding search of cellular telephone "purely investigatory" and thus not lawful inventory search). Even assuming that standard procedures authorized such a search, the legitimate purposes served by inventory searches in the physical world do not translate well into the intangible realm. Information does not generally need to be reviewed to be protected and does not pose a risk of physical danger. Although an owner could claim that his computer files were altered or deleted while in police custody, an officer's examination of the contents of the files would offer little protection from tampering. Accordingly, agents will generally need to obtain a search warrant in order to examine seized computer files held in custody unless some other exception to the warrant requirement applies.

6. Border Searches

In order to protect the government's ability to monitor contraband and other property that may enter or exit the United States illegally, the Supreme Court has recognized a special exception to the warrant requirement for searches that occur at the border of the United States (or at the border's functional equivalent). According to the Court, routine searches at the border do not require a warrant, probable cause, or even reasonable suspicion that the search may uncover contraband or evidence. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Searches that are especially intrusive, however, require at least reasonable suspicion. *See id.* at 541. These rules apply to people and property both entering and exiting the United States. *See United States v. Oriakhi*, 57 F.3d 1290, 1297 (4th Cir. 1995).

The Supreme Court's most recent border search case, *United States v. Flores-Montano*, 541 U.S. 149 (2004), suggests that reasonable suspicion is not required for most non-destructive border searches of property. In *Flores-Montano*, the Court determined that the border search of an automotive fuel tank did not require reasonable suspicion. The Court explained that "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles." *Id.* at 1585. Although there may be a lesser privacy interest in gas tanks than in other property (such as computers), the Court's analysis in *Flores-Montano* does not appear to be narrowly confined to gas tanks or vehicles. In response to the defendant's argument that the Fourth Amendment protects property as much as privacy, the Court emphasized the lack of physical damage to the gas tank and concluded that "[w]hile it may be true that some searches of property are so destructive as to require a different result, this was not one of them." *Id.* at 1587. One appellate court has noted that "[t]he Supreme Court recently made clear that reasonable suspicion is usually not required for officers to conduct non-destructive border searches of property." *United States v. Camacho*, 368 F.3d 1182, 1183 (9th Cir. 2004).

Since *Flores-Montano*, courts have upheld suspicionless border searches of computers. In *United States v. Arnold*, 523 F.3d 941, 946 (9th Cir. 2008), the Ninth Circuit held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices." In so holding, the *Arnold* court explicitly rejected the defendant's argument, previously adopted by the district court, that searching a laptop is more

"intrusive" than a typical search of property and more like searching a home because of its large storage capacity. Instead, the *Arnold* court found no logical distinction between a suspicionless border search of a traveler's luggage and a similar suspicionless search of a laptop. *See id.* at 947. *See also United States v. Hampe*, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) (rejecting the *Arnold* district court analysis and holding that border search of computer files did not require reasonable suspicion); *United States v. Romm*, 455 F.3d 990, 996-97 (9th Cir. 2006) (upholding border search of computer and suggesting, but not holding, that reasonable suspicion is not required for non-destructive property searches at the border).

In *United States v. Ickes*, 393 F.3d 501, 506-07 (4th Cir. 2005), the Fourth Circuit also held that a search of a computer and disks within the defendant's car was permissible under the border search exception, emphasizing the breadth of the government's border search authority. The *Ickes* court did not address whether the search of the defendant's car, and the computer and disks it contained, was "routine." However, the court did note that, while most searches of computers at the border would likely result from reasonable suspicion, it would not "enthron[e] this notion as a matter of constitutional law." *Id.* at 507. *See also United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."). In addition, *Ickes* rejected the defendant's argument that border searches of computers should be limited based on computers' storage of expressive materials. *Ickes*, 359 F.3d at 506. *See also Arnold*, 523 F.3d at 948 (following *Ickes* and refusing to carve out a First Amendment exception to the border search doctrine).

In two pre-*Flores-Montano* cases, district courts upheld warrantless searches of computer disks for contraband computer files, finding that the searches were "routine" and did not require reasonable suspicion. In *United States v. Irving*, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003), the court noted that "any other decision effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search." On appeal, after *Flores-Montano*, the Second Circuit upheld the district court's denial of Irving's motion to suppress. *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006). However, because the Second Circuit found that the customs agents who searched Irving had reasonable suspicion, it did not consider whether reasonable suspicion was required. *Id.* at 124. Similarly, in *United States v.*

Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000), *aff'd on other grounds*, 274 F.3d 1007 (5th Cir. 2001), the court held that a search of the defendant's computer and floppy disks was a routine search for which no suspicion was required. *See id*. at 688. On appeal, the Fifth Circuit affirmed on other grounds and did not reach the issue of whether the seizure of the defendant's computer equipment could be considered routine. *See Roberts*, 274 F.3d at 1017.

7. Probation and Parole

Individuals on probation, parole, or supervised release enjoy a diminished expectation of privacy and may be subject to warrantless searches based on reasonable suspicion, or, potentially, without any particularized suspicion. In *United States v. Knights*, 534 U.S. 112, 122 (2001), the Supreme Court considered the validity of a warrantless search based on reasonable suspicion of a probationer's home where the conditions of the probation required the probationer to submit to a search at any time, with or without a warrant or reasonable cause. The Court did not rely on the "special needs" analysis of *Griffin v. Wisconsin*, 483 U.S. 868 (1987), a previous probation search case. Instead, the Court employed "ordinary Fourth Amendment analysis that considers all the circumstances of a search." *Knights*, 534 U.S. at 122. The Court noted the probationer's diminished expectation of privacy, the government's interests in preventing recidivism and reintegrating probationers into the community, and the government's concern that probationers are more likely to commit (and conceal) crime than ordinary citizens. *See id.* at 120-21. Balancing these factors, the Court found that the search required "no more than reasonable suspicion." *Id.* at 121.

In *Samson v. California*, 547 U.S. 843, 857 (2006), the Supreme Court extended *Knights*, holding that the Fourth Amendment does not prohibit a *suspicionless* search of a parolee. As in *Knights*, the Court employed a "totality of the circumstances" approach and considered the parole agreement that unambiguously allowed for suspicionless searches, the government's interests in supervising parolees, and the government's interest in reducing recidivism. *See Samson*, 547 U.S. at 852-53. However, the Court in *Samson* did not make clear whether its holding extended to probationers, and the Court noted that parolees have "fewer expectations of privacy than probationers." *Id.* at 850; *see also United States v. Herndon*, 501 F.3d 683, 688 n.2 (6th Cir. 2007) (noting that *Samson*'s application to probationers is unclear).

Following *Knights* and *Samson*, the Sixth Circuit upheld a warrantless search of a probationer's computer based on reasonable suspicion that the probationer had violated his probation by using the Internet. *See United States v. Herndon*, 501 F.3d 683, 692 (6th Cir. 2007). Herndon, on probation for sexual exploitation of a minor, was subject to a specific condition prohibiting him from using the Internet and requiring him to allow his probation officer to search his computer at any time for Internet use. *See id.* at 685. After Herndon told his probation officer that he had used the Internet to search for a job, the probation officer went to Herndon's residence and searched his computer and an external hard drive, ultimately finding child pornography. While finding that the probation condition did not meet the "special need" standard of *Griffin* because it did not itself specifically include a reasonable suspicion requirement, the court nevertheless found the search was "reasonable" under *Knights*: Herndon's reasonable expectation of privacy was "dramatically reduced" by the probation condition and was outweighed by the government's interest in preventing recidivism. *Id.* at 689-91. The Sixth Circuit concluded that the probation officer's search was proper, as it required "no more than reasonable suspicion." *Id.* at 691.

At least one court has upheld the warrantless search of a probationer's computer even in the absence of an explicit probation condition requiring the probationer to submit to a warrantless search. In *United States v. Yuknavich*, 419 F.3d 1302, 1311 (11th Cir. 2005), probationer Yuknavich had been convicted of child pornography-related charges. While his probation did not include a warrantless search provision, it did prohibit him from using the Internet, except for work purposes during work hours. During a routine home visit, Yuknavich's probation officers observed a computer connected to a modem, examined it, and discovered that Yuknavich had been downloading child pornography. The Court held that even in the absence of a provision in his probation agreement authorizing warrantless searches, Yuknavich's expectation of privacy in his computer was diminished by the condition specifically restricting his Internet access, especially in light of the crime for which he was on probation. *See id.* at 1310. Thus, the court followed *Knights* and held that the search of Yuknavich's computer required, at most, reasonable suspicion. *See id.* at 1311.

D. Special Case: Workplace Searches

Workplace searches occur often in computer cases, as workplace computers frequently store evidence of criminal activity. Whether such searches require a warrant depends on several factual distinctions, beginning with whether the workplace is in the public sector or the private sector. In general, law enforcement officers can conduct a warrantless search of private (*i.e.*, non-government) workplaces only if the officers obtain the consent of either the employer or an employee with common authority over the area searched. For government workplaces, the inquiry into whether a warrant is required to conduct a workplace search is based on the "special needs" framework set forth in *O'Connor v. Ortega*, 480 U.S. 709 (1987). Under that framework, a government employee may, depending on circumstances, enjoy a reasonable expectation of privacy in his workplace. However, even when the employee has a reasonable expectation of privacy, employers can nevertheless conduct warrantless searches provided the searches are work-related, justified at their inception, and permissible in scope. *Id.* at 725-26.

One cautionary note is in order here. This discussion evaluates the legality of warrantless workplace searches of computers under the Fourth Amendment. In many cases, however, workplace searches will implicate federal privacy statutes in addition to the Fourth Amendment. For example, efforts to obtain an employee's files and email from the employer's network server raise issues under the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (discussed in Chapter 3), and workplace monitoring of an employee's Internet use may implicate Title III, 18 U.S.C. §§ 2510-2522 (discussed in Chapter 4). Before conducting a workplace search, investigators must make sure that their search will not violate either the Fourth Amendment or relevant federal privacy statutes. Investigators should contact CCIPS at (202) 514-1026 or the CHIP in their district (*see* Introduction, p. xii) for further assistance.

1. Private-Sector Workplace Searches

The rules for conducting warrantless searches and seizures in private-sector workplaces generally mirror the rules for conducting warrantless searches in homes and other personal residences. Private company employees generally retain a reasonable expectation of privacy in their workplaces. As a result, searches by law enforcement of a private workplace will usually require a warrant unless the agents obtain the consent of an employer or a co-worker with common authority.

a. Reasonable Expectation of Privacy in Private-Sector Workplaces

Private-sector employees will usually retain a reasonable expectation of privacy in their office space. In *Mancusi v. DeForte*, 392 U.S. 364, 365 (1968), police officers conducted a warrantless search of an office at a local union headquarters that defendant Frank DeForte shared with several other union officials. In response to DeForte's claim that the search violated his Fourth Amendment rights, the police officers argued that the joint use of the space by DeForte's co-workers made his expectation of privacy unreasonable. The Court disagreed, stating that DeForte "still could reasonably have expected that only [his officemates] and their personal or business guests would enter the office, and that records would not be touched except with their permission or that of union higher-ups." *Id.* at 369. Because only a specific group of people actually enjoyed joint access and use of DeForte's office, the officers' presence violated DeForte's reasonable expectation of privacy. *See id. See also United States v. Most*, 876 F.2d 191, 198 (D.C. Cir. 1989) ("[A]n individual need not shut himself off from the world in order to retain his fourth amendment rights. He may invite his friends into his home but exclude the police; he may share his office with co-workers without consenting to an official search."); *United States v. Lyons*, 706 F.2d 321, 325 (D.C. Cir. 1983) ("One may freely admit guests of one's choosing—or be legally obligated to admit specific persons—without sacrificing one's right to expect that a space will remain secure against all others."). As a practical matter, then, private employees will generally retain an expectation of privacy in their work space unless that space is "open to the world at large." *Id.* at 326.

Some courts have held that a private-sector employee has no reasonable expectation of privacy in the contents of his work computer or email account when his employer has explicitly reserved the right to monitor the employee's computer use or search his computer files. *See United States v. Bailey*, 272 F. Supp. 2d 822, 835-36 (D. Neb. 2003); *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002). However, these cases rely on precedents from the public-sector context without considering the distinction between private and public employers. For example, the fact that a private employer reserves the right to search an employee's computer should not imply that the government can seize the computer without a warrant, absent the employer consenting or conducting a private search. Prosecutors should be wary in relying on these cases. For example, in *United States v. Ziegler*, 456 F.3d 1138, 1144-46 (9th Cir. 2006), the Ninth Circuit initially held that a private-sector employee had

no reasonable expectation of privacy in his workplace computer based on his employer's monitoring and computer use policy. However, this opinion was withdrawn and superseded by *United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007), in which the court, relying on *Mancusi v. DeForte*, held that the employee in fact retained a reasonable expectation of privacy in his workplace computer.

b. Consent in Private-Sector Workplaces

Although most non-government workplaces will support a reasonable expectation of privacy from a law enforcement search, agents can defeat this expectation by obtaining the consent of a party who exercises common authority over the area searched. *See Matlock*, 415 U.S. at 171. In practice, this means that agents can often overcome the warrant requirement by obtaining the consent of the target's employer or supervisor. Depending on the facts, a co-worker's consent may suffice as well.

Private-sector employers and supervisors generally enjoy a broad authority to consent to searches in the workplace. For example, in *United States v. Gargiso*, 456 F.2d 584 (2d Cir. 1972), a pre-*Matlock* case, agents conducting a criminal investigation of an employee of a private company sought access to a locked, wired-off area in the employer's basement. The agents explained their needs to the company's vice-president, who took the agents to the basement and opened the basement with his key. When the employee attempted to suppress the evidence that the agents discovered in the basement, the court held that the vice-president's consent was effective. Because the vice-president shared supervisory power over the basement with the employee, the court reasoned, he could consent to the agents' search of that area. *See id.* at 586-87. *See also United States v. Bilanzich*, 771 F.2d 292, 296-97 (7th Cir. 1985) (holding that the owner of a hotel could consent to search of locked room used by hotel employee to store records, even though owner did not carry a key, because employee worked at owner's bidding); *J.L. Foti Constr. Co. v. Donovan*, 786 F.2d 714, 716-17 (6th Cir. 1986) (per curiam) (holding that a general contractor's superintendent could consent to an inspection of an entire construction site, including subcontractor's work area).

In most cases, private-sector employers will retain sufficient authority over workplace computers to consent to a government search of the computers. In *United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir. 2007), the court held that an employer could consent to a search of the computer it provided to an

employee, explaining that "the computer is the type of workplace property that remains within the control of the employer 'even if the employee has placed personal items in [it].'" The court also noted the existence of a workplace policy and practice of monitoring employee computer use. *See id.* In a close case, an employment policy or computer network banner that establishes the employer's right to consent to a workplace search can help establish the employer's common authority to consent under *Matlock*. For more information on banners, *see* Appendix A.

When co-workers exercise common authority over a workspace, investigators can rely on a co-worker's consent to search that space. For example, in *United States v. Buettner-Janusch*, 646 F.2d 759 (2d Cir. 1981), a professor and an undergraduate research assistant at New York University consented to a search of an NYU laboratory managed by a second professor suspected of using his laboratory to manufacture LSD and other drugs. Although the search involved opening vials and several other closed containers, the Second Circuit held that *Matlock* authorized the search because both consenting co-workers had been authorized to make full use of the lab for their research. *See id.* at 765-66. *See also United States v. Jenkins*, 46 F.3d 447, 455-58 (5th Cir. 1995) (allowing an employee to consent to a search of the employer's property); *United States v. Murphy*, 506 F.2d 529, 530 (9th Cir. 1974) (per curiam) (same); *United States v. Longo*, 70 F. Supp. 2d 225, 256 (W.D.N.Y. 1999) (allowing secretary to consent to search of employer's computer). *But see United States v. Buitrago Pelaez*, 961 F. Supp. 64, 67-68 (S.D.N.Y. 1997) (holding that a receptionist could consent to a general search of the office, but not of a locked safe to which receptionist did not know the combination).

c. Employer Searches in Private-Sector Workplaces

Warrantless workplace searches by private employers rarely violate the Fourth Amendment. So long as the employer is not acting as an instrument or agent of the Government at the time of the search, the search is a private search and the Fourth Amendment does not apply. *See Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989).

2. Public-Sector Workplace Searches

Although warrantless computer searches in private-sector workplaces follow familiar Fourth Amendment rules, the application of the Fourth Amendment to public-sector workplace searches of computers presents a different matter. In *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Supreme Court introduced

a distinct framework for evaluating warrantless searches in government workplaces, a framework that applies to computer searches. According to *O'Connor*, a government employee can enjoy a reasonable expectation of privacy in his workplace. *See id.* at 717 (O'Connor, J., plurality opinion); *id.* at 730 (Scalia, J., concurring). However, an expectation of privacy becomes unreasonable if "actual office practices and procedures, or . . . legitimate regulation" permit the employee's supervisor, co-workers, or the public to enter the employee's workspace. *Id.* at 717 (O'Connor, J., plurality opinion). Further, employers can conduct "reasonable" warrantless searches even if the searches violate an employee's reasonable expectation of privacy. Such searches include work-related, noninvestigatory intrusions (*e.g.*, entering an employee's locked office to retrieve a file) and reasonable investigations into work-related misconduct. *See id.* at 725-26 (O'Connor, J., plurality opinion); *id.* at 732 (Scalia, J., concurring).

a. Reasonable Expectation of Privacy in Public Workplaces

The reasonable expectation of privacy test formulated by the *O'Connor* plurality asks whether a government employee's workspace is "so open to fellow employees or to the public that no expectation of privacy is reasonable." *O'Connor*, 480 U.S. at 718 (plurality opinion). This standard differs significantly from the standard analysis applied in private workplaces. Whereas private-sector employees enjoy a reasonable expectation of privacy in their workspace unless the space is "open to the world at large," *Lyons*, 706 F.2d at 326, government employees retain a reasonable expectation of privacy in the workplace only if a case-by-case inquiry into "actual office practices and procedures" shows that it is reasonable for employees to expect that others will not enter their space. *See O'Connor*, 480 U.S. at 717 (plurality opinion); *Rossi v. Town of Pelham*, 35 F. Supp. 2d. 58, 63-64 (D.N.H. 1997). *See also O'Connor*, 480 U.S. at 730-31 (Scalia, J., concurring) (noting the difference between the expectation-of-privacy analysis offered by the *O'Connor* plurality and that traditionally applied in private workplace searches). From a practical standpoint, then, public employees are less likely to retain a reasonable expectation of privacy against government searches at work than are private employees.

Courts evaluating public employees' reasonable expectation of privacy in the wake of *O'Connor* have considered the following factors: whether the work area in question is assigned solely to the employee; whether others have access to the space; whether the nature of the employment requires a close working

relationship with others; whether office regulations place employees on notice that certain areas are subject to search; and whether the property searched is public or private. *See Vega-Rodriguez v. Puerto Rico Tel. Co.*, 110 F.3d 174, 179-80 (1st Cir. 1997) (summarizing cases); *United States v. Mancini*, 8 F.3d 104, 109 (1st Cir. 1993). In general, the courts have rejected claims of an expectation of privacy in an office when the employee knew or should have known that others could access the employee's workspace. *See, e.g.*, *United States v. King*, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (contractor had no reasonable expectation of privacy in "shared" files accessible by entire military base computer network); *United States v. Barrows*, 481 F.3d 1246, 1248-49 (10th Cir. 2007) (public employee had no reasonable expectation of privacy in his own computer in workplace when he left computer out and unprotected from use by others); *Sheppard v. Beerman*, 18 F.3d 147, 152 (2d Cir. 1994) (judge's search through his law clerk's desk and file cabinets did not violate the clerk's reasonable expectation of privacy because of the clerk's close working relationship with the judge); *Schowengerdt v. United States*, 944 F.2d 483, 488 (9th Cir. 1991) (civilian engineer employed by the Navy who worked with classified documents at an ordinance plant had no reasonable expectation of privacy in his office because investigators were known to search employees' offices for evidence of misconduct on a regular basis). *But see United States v. Taketa*, 923 F.2d 665, 673 (9th Cir. 1991) (concluding that public employee retained expectation of privacy in office shared with several co-workers). In contrast, the courts have found that a search violates a public employee's reasonable expectation of privacy when the employee had no reason to expect that others would access the space searched. *See O'Connor*, 480 U.S. at 718-19 (plurality) (physician at state hospital retained expectation of privacy in his desk and file cabinets where there was no evidence that other employees could enter his office and access its contents); *Rossi*, 35 F. Supp. 2d at 64 (holding that town clerk enjoyed reasonable expectation of privacy in 8' x 8' office that the public could not access and other town employees did not enter).

While agents must evaluate whether a public employee retains a reasonable expectation of privacy in the workplace on a case-by-case basis, official written employment policies can simplify the task dramatically. *See O'Connor*, 480 U.S. at 717 (plurality) ("legitimate regulation" of the work place can reduce public employees' Fourth Amendment protections). Courts have uniformly deferred to public employers' official policies that expressly authorize access to the employee's workspace and have relied on such policies when ruling that the employee does not retain a reasonable expectation of privacy in the workplace.

See American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Serv., 871 F.2d 556, 559-61 (6th Cir. 1989) (postal employees retained no reasonable expectation of privacy in contents of government lockers after signing waivers stating that lockers were subject to inspection at any time, even though lockers contained personal items); *United States v. Bunkers*, 521 F.2d 1217, 1219-1221 (9th Cir. 1975) (same, noting language in postal manual stating that locker is "subject to search by supervisors and postal inspectors"). Of course, whether a specific policy eliminates a reasonable expectation of privacy is a factual question. Employment policies that do not explicitly address employee privacy may prove insufficient to eliminate Fourth Amendment protection. *See, e.g.*, *Taketa*, 923 F.2d at 672-73 (concluding that regulation requiring DEA employees to "maintain clean desks" did not defeat workplace expectation of privacy of non-DEA employee assigned to DEA office).

☞ When planning to search a government computer in a government workplace, agents should look for official employment policies or computer log on "banners" that can eliminate a reasonable expectation of privacy in the computer.

Written employment policies and computer log on "banners" are particularly important in cases that consider whether government employees enjoy a reasonable expectation of privacy in government computers. Banners are written notices that greet users before they log on to a computer or computer network; they can inform users of the privacy rights that they do or do not retain in their use of the computer or network. *See generally* Appendix A.

In general, government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no reasonable expectation of privacy in the information stored there. For example, in *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), computer specialists at a division of the Central Intelligence Agency learned that an employee named Mark Simons had been using his desktop computer at work to obtain pornography available on the Internet, in violation of CIA policy. The computer specialists accessed Simons' computer remotely without a warrant, and obtained copies of over a thousand picture files that Simons had stored on his hard drive. Many of these picture files contained child pornography, which were turned over to law enforcement. When Simons filed a motion to suppress the fruits of the remote search of his hard drive, the Fourth Circuit held that the CIA division's official Internet usage policy

eliminated any reasonable expectation of privacy that Simons might otherwise have in the copied files. *See id.* at 398. The policy stated that the CIA division would "periodically audit, inspect, and/or monitor [each] user's Internet access as deemed appropriate," and that such auditing would be implemented "to support identification, termination, and prosecution of unauthorized activity." *Id.* at 395-96. Simons did not deny that he was aware of the policy. *See id*. at 398 n.8. In light of the policy, the Fourth Circuit held, Simons did not retain a reasonable expectation of privacy "with regard to the record or fruits of his Internet use," including the files he had downloaded. *Id.* at 398.

Other courts have agreed with the approach articulated in *Simons* and have held that banners and policies generally eliminate a reasonable expectation of privacy in contents stored in a government employee's network account. *See Biby v. Board of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (university policy stating that computer files and emails may be searched in response to litigation discovery requests eliminated computer user's reasonable expectation of privacy); *United States v. Thorn*, 375 F.3d 679, 683 (8th Cir. 2004) (computer use policy eliminated employee's reasonable expectation of privacy in computer); *United States v. Angevine*, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (banner and computer policy eliminated a public employee's reasonable expectation of privacy in data downloaded from Internet); *United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 2000) (Air Force sergeant did not have a reasonable expectation of privacy in his government email account because email use was reserved for official business and network banner informed each user upon logging on to the network that use was subject to monitoring); *Wasson v. Sonoma County Junior College Dist.*, 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (public employer's computer policy giving the employer "the right to access all information stored on [the employer's] computers" defeats an employee's reasonable expectation of privacy in files stored on employer's computers); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (police officers did not retain a reasonable expectation of privacy in their use of a pager system, in part because the Chief of Police had issued an order announcing that all messages would be logged). *But see DeMaine v. Samuels*, 2000 WL 1658586, at *7 (D. Conn. Sept. 25, 2000) (suggesting that the existence of an employment manual explicitly authorizing searches "weighs heavily" in the determination of whether a government employee retained a reasonable expectation of privacy at work, but "does not, on its own, dispose of the question"). Conversely, a court may note the absence of a banner or computer policy in finding that an employee has a reasonable expectation of

privacy in the use of his computer. *See United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *aff'd*, 359 F.3d 356, 358 (5th Cir. 2004); *Leventhal v. Knapek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (noting that agency had not placed employee on notice that he had no expectation of privacy in his computer).

Of course, whether a specific policy eliminates a reasonable expectation of privacy is a factual question. Agents and prosecutors must consider whether a given policy is broad enough to reasonably contemplate the search to be conducted. If the policy is narrow, it may not waive the government employee's reasonable expectation of privacy against the search that the government plans to execute. For example, in *Simons*, the Fourth Circuit concluded that although the CIA division's Internet usage policy eliminated Simons' reasonable expectation of privacy in the fruits of his Internet use, it did *not* eliminate his reasonable expectation of privacy in the physical confines of his office. *See Simons*, 206 F.3d at 399 n.10. Accordingly, the policy by itself was insufficient to justify a physical entry into Simons' office. *See id.* at 399. *See also Taketa*, 923 F.2d at 672-73 (concluding that regulation requiring DEA employees to "maintain clean desks" did not defeat workplace expectation of privacy of non-DEA employee assigned to DEA office). In addition, *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), supplies an example of a court interpreting a banner very narrowly. In *Long*, a Department of Defense banner warned users that the government could monitor the computer system "for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures. . . ." The court held that a user maintained a reasonable expectation of privacy in her email, stating that the "banner described access to 'monitor' the computer system, not to engage in law enforcement intrusions by examining the contents of particular emails in a manner unrelated to maintenance of the e-mail system." *Id.* at 63. However, in a subsequent case before the same court with a similar computer banner, the court declined to follow *Long*. *See United States v. Larson*, 66 M.J. 212, 216 (2008) (finding no expectation of privacy in government computer where banner established consent to monitor). Sample banners appear in Appendix A.

Furthermore, courts may consider whether or how the employer actually enforces its policy when deciding whether the policy eliminates an employee's expectation of privacy. For example, in *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), a city employee had signed a computer use

policy acknowledging that he had no expectation of privacy in his use of the pager provided to him by the city. Although the court noted that this policy would eliminate the employee's reasonable expectation policy "[i]f that were all," *id.* at 906, the court nevertheless found that the employee had a reasonable expectation of privacy because of an "informal policy that the text messages would not be audited" if the employee paid any charges incurred through his use of text messaging for non-official purposes. *Id. See also Long*, 64 M.J. at 64 (noting network administrator's testimony that he did not monitor individual email accounts when testing or monitoring the network).

b. "Reasonable" Workplace Searches Under O'Connor v. Ortega

☞ Government employers and their agents can conduct "reasonable" work-related searches without a warrant even if those searches violate an employee's reasonable expectation of privacy.

In most circumstances, a warrant must be obtained before a government actor can conduct a search that violates an individual's reasonable expectation of privacy. In the context of government employment, however, the government's role as an employer (as opposed to its role as a law-enforcer) presents a special case. In *O'Connor*, the Supreme Court held that a public employer or the employer's agent can conduct a workplace search that violates a public employee's reasonable expectation of privacy so long as the search is "reasonable." *See O'Connor*, 480 U.S. at 722-23 (plurality); *id.* at 732 (Scalia, J., concurring). The Court's decision adds public workplace searches by employers to the list of "special needs" exceptions to the warrant requirement. The "special needs" exceptions permit the government to dispense with the usual warrant requirement when its officials infringe upon protected privacy rights in the course of acting in a non-law enforcement capacity. *See, e.g.*, *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (applying the "special needs" exception to permit public school officials to search student property without a warrant in an effort to maintain discipline and order in public schools); *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 677 (1989) (applying the "special needs" exception to permit warrantless drug testing of Customs employees who seek promotions to positions where they would handle sensitive information). In these cases, the Court has held that the need for government officials to pursue legitimate non-law-enforcement aims justifies a relaxing of the warrant requirement because "the burden of obtaining a warrant is likely to frustrate the [non-law-enforcement] governmental purpose

behind the search." *O'Connor*, 480 U.S. at 720 (quoting *Camara v. Municipal Court*, 387 U.S. 523, 533 (1967)).

According to *O'Connor*, a warrantless search must satisfy two requirements to qualify as "reasonable." First, the employer or his agents must participate in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings. Second, the search must be justified at its inception and permissible in its scope.

i. The Search Must Be Work-Related

The first element of *O'Connor*'s reasonableness test requires that the employer or his agents must participate in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings. *See O'Connor*, 480 U.S. at 721. This element limits the *O'Connor* exception to circumstances in which the government actors who conduct the search act in their capacity as employers, rather than law enforcers. The *O'Connor* Court specified two such circumstances. First, the Court concluded that public employers can conduct reasonable work-related noninvestigatory intrusions, such as entering an employee's office to retrieve a file or report while the employee is out. *See id.* at 721-22 (plurality); *id.* at 732 (Scalia, J., concurring). Second, the Court concluded that employers can conduct reasonable investigations into an employee's work-related misconduct, such as entering an employee's office to investigate employee misfeasance that threatens the efficient and proper operation of the office. *See id.* at 724 (plurality); *id.* at 732 (Scalia, J., concurring).

The line between a legitimate work-related search and an illegitimate search for criminal evidence is clear in theory, but often blurry in fact. Public employers who learn of misconduct at work may investigate it with dual motives: they may seek evidence both to root out "inefficiency, incompetence, mismanagement, or other work-related misfeasance," *id.* at 724, and also to collect evidence for a criminal prosecution. Indeed, the two categories may merge altogether. For example, government officials who have criminal investigators under their command may respond to allegations of work-related misconduct by directing the investigators to search employee offices for evidence of a crime.

The courts have adopted fairly generous interpretations of *O'Connor* when confronted with mixed-motive searches. In general, the presence and involvement of law enforcement officers will not invalidate the search so long as the employer or his agent participates in the search for legitimate work-

related reasons. *See, e.g.*, *United States v. Slanina*, 283 F.3d 670, 678-79 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *aff'd*, 359 F.3d 356, 358 (5th Cir. 2004) (approving search by official in charge of fire and police departments and stating that "*O'Connor*'s goal of ensuring an efficient workplace should not be frustrated simply because the same misconduct that violates a government employer's policy also happens to be illegal"); *Gossmeyer v. McDonald*, 128 F.3d 481, 492 (7th Cir. 1997) (presence of law enforcement officers in a search team looking for evidence of work-related misconduct does not transform search into an illegitimate law enforcement search); *Taketa*, 923 F.2d at 674 (search of DEA office space by DEA agents investigating allegations of illegal wiretapping "was an internal investigation directed at uncovering work-related employee misconduct."); *Shields v. Burge*, 874 F.2d 1201, 1202-05 (7th Cir. 1989) (applying the *O'Connor* exception to an internal affairs investigation of a police sergeant that paralleled a criminal investigation); *Ross v. Hinton*, 740 F. Supp. 451, 458 (S.D. Ohio 1990) (a public employer's discussions with law enforcement officer concerning employee's alleged criminal misconduct, culminating in officer's advice to "secure" the employee's files, did not transform employer's subsequent search of employee's office into a law enforcement search).

Although the presence of law enforcement officers ordinarily will not invalidate a work-related search, a few courts have indicated that whether *O'Connor* applies depends as much on the identity of the personnel who conduct the search as whether the purpose of the search is work-related. For example, in *United States v. Simons*, 206 F.3d 392, 400 (4th Cir. 2000), the Fourth Circuit concluded that *O'Connor* authorized the search of a government employee's office by his supervisor even though the dominant purpose of the search was to uncover evidence of a crime. Because the search was work-related and conducted by the employee's supervisor, the Court indicated, it fell within the scope of *O'Connor*. *See id.* ("[The employer] did not lose its special need for the efficient and proper operation of the workplace merely because the evidence obtained was evidence of a crime." (internal quotation marks and citations omitted)). Conversely, one district court has held that the *O'Connor* exception did not apply when a government employer sent a uniformed police officer to an employee's office, even though the purpose of the police officer's presence was entirely work-related. *See Rossi v. Town of Pelham*, 35 F. Supp. 2d 58, 65-66 (D.N.H. 1997) (in civil action pursuant to 42 U.S.C. § 1983, concluding that *O'Connor* exception did not apply when town officials sent a single police officer to town clerk's office to ensure that clerk did not remove public records

from her office before a scheduled audit could occur; the resulting search was a "police intrusion" rather than an "employer intrusion").

Of course, courts will invalidate warrantless workplace searches when the facts establish that law enforcement provided the real reason for the search, and the search violated an employee's reasonable expectation of privacy. *See United States v. Hagarty*, 388 F.2d 713, 717 (7th Cir. 1968) (surveillance installed by criminal investigators violated the Fourth Amendment where purpose of surveillance was "to detect criminal activity" rather than "to supervise and investigate" a government employee); *United States v. Kahan*, 350 F. Supp. 784, 791 (S.D.N.Y. 1972) (invalidating warrantless search of INS employee's wastebasket by INS criminal investigator who searched the employee's wastebasket for evidence of a crime every day after work with the employer's consent), *rev'd in part on other grounds*, 479 F.2d 290 (2d Cir. 1973), *rev'd with directions to reinstate the district court judgment*, 415 U.S. 239 (1974).

ii. The Search Must Be Justified At Its Inception and Permissible In Its Scope

To be "reasonable" under the Fourth Amendment, a work-related employer search of the type endorsed in *O'Connor* must also be both "justified at its inception" and "permissible in its scope." *O'Connor*, 480 U.S. at 726 (plurality). A search will be justified at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose." *Id. See, e.g.*, *Simons*, 206 F.3d at 401 (entrance into employee's office to seize his computer was justified at its inception because employer knew that employee had used the computer to download child pornography); *Gossmeyer*, 128 F.3d at 491 (co-worker's specific allegations of serious misconduct made Sheriff's search of Child Protective Investigator's locked desk and file cabinets justified at its inception); *Taketa*, 923 F.2d at 674 (report of misconduct justified initial search of employee's office); *Shields*, 874 F.2d at 1204 (suggesting in dicta that search of police officer's desk for narcotics pursuant to internal affairs investigation might be reasonable following an anonymous tip); *DeMaine v. Samuels*, 2000 WL 1658586, at *10 (D. Conn. Sept. 25, 2000) (search of police officer's day planner was justified by information from two reliable sources that the officer kept detailed attendance notes relevant to overtime investigation involving other officers); *Williams v. Philadelphia Housing Auth.*, 826 F. Supp. 952, 954 (E.D. Pa. 1993) (employee's search for a computer disk in employee's office was

justified at its inception because employer needed contents of disk for official purposes). *But see Wiley v. Department of Justice*, 328 F.3d 1346, 1356-57 (Fed. Cir. 2003) (search of employee's car based on ten-month-old anonymous tip was not justified); *Ortega v. O'Connor*, 146 F.3d 1149, 1162 (9th Cir. 1998) (vague, uncorroborated and stale complaints of misconduct do not justify a decision to search an employee's office). A search will be "permissible in its scope" when "the measures adopted are reasonably related to the objectives of the search and [are] not excessively intrusive in light of the nature of the misconduct." *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted). This standard requires employers and their agents to tailor work-related searches to the alleged misfeasance. *See, e.g.*, *Leventhal v. Knapek*, 266 F.3d 64, 75-77 (2d Cir. 2001) (search for the presence of non-agency-approved software on employee's computer was not excessively intrusive because officials searched only file names at first and then searched only suspicious directories on subsequent visits); *Simons*, 206 F.3d at 401 (search for child pornography believed to be stored in employee's computer was permissible in scope because individual who conducted the search "simply crossed the floor of [the defendant's] office, switched hard drives, and exited"); *Gossmeyer*, 128 F.3d at 491 (workplace search for images of child pornography was permissible in scope because it was limited to places where such images would likely be stored); *Samuels*, 2000 WL 1658586, at *10 (search through police officer's day planner was reasonable because Internal Affairs investigators had reason to believe day planner contained information relevant to investigation of overtime abuse). If employers conduct a search that unreasonably exceeds the scope necessary to pursue the employer's legitimate work-related objectives, the search will be "unreasonable" and will violate the Fourth Amendment. *See O'Connor*, 146 F.3d at 1163 ("a general and unbounded" search of an employee's desk, cabinets, and personal papers was impermissible in scope where the search team did not attempt to limit their investigation to evidence of alleged misconduct); *Narducci v. Village of Bellwood*, 444 F. Supp. 2d 924, 932 (N.D. Ill. 2006) (purpose of addressing threats to employees did not justify recording all employee phone calls, without notice to employees, for six years after complaints of threats had stopped).

c. Consent in Public-Sector Workplaces

Although public employers may search employees' workplaces without a warrant for work-related reasons, public workplaces offer a more restrictive milieu in one respect. In government workplaces, employers acting in their

official capacity generally cannot consent to a law enforcement search of their employees' offices. *See United States v. Blok*, 188 F.2d 1019, 1021 (D.C. Cir. 1951) (a government supervisor cannot consent to a law enforcement search of a government employee's desk); *Taketa*, 923 F.2d at 673; *Kahan*, 350 F. Supp. at 791. The rationale for this result is that the Fourth Amendment cannot permit one government official to consent to a search by law enforcement that he could not conduct himself. *See Blok*, 188 F.2d at 1021 ("Operation of a government agency and enforcement of criminal law do not amalgamate to give a right of search beyond the scope of either."). Accordingly, law enforcement searches conducted pursuant to a public employer's consent must be evaluated under *O'Connor* rather than the third-party consent rules of *Matlock*. The question in such cases is not whether the public employer had common authority to consent to the search, but rather whether the combined law enforcement and employer search satisfied the Fourth Amendment standards of *O'Connor v. Ortega*.

E. International Issues

Increasingly, electronic evidence necessary to prevent, investigate, or prosecute a crime may be located outside the borders of the United States. This can occur for several reasons. Criminals can use the Internet to commit or facilitate crimes remotely, *e.g.*, when Russian hackers steal money from a bank in New York, or when the kidnappers of an American citizen deliver demands by email for release of their captive. Communications also can be "laundered" through third countries, such as when a criminal in Brooklyn uses the Internet to pass a communication through Tokyo, Tel Aviv, and Johannesburg before it reaches its intended recipient in Manhattan—much the way money can be laundered through banks in different countries in order to hide its source. In addition, provider architecture may route or store communications in the country where the provider is based, regardless of the location of its users.

When United States authorities investigating a crime believe electronic evidence is stored by an Internet service provider on a computer located abroad (in "Country A"), U.S. law enforcement usually must seek assistance from law enforcement authorities in Country A. Because, in general, law enforcement officers exercise their functions in the territory of another country only with the consent of that country, U.S. law enforcement should only make direct contact with an ISP located in Country A with (1) prior permission of the foreign government; (2) approval of DOJ's Office of International Affairs ("OIA")

(which would know of particular sensitivities and accepted practices); or (3) other clear indicia that such practice would not be objectionable in Country A. The U.S. view (and that of some other countries) is that prior consultation is not required to (1) access publicly available materials in Country A, such as those posted to a public website, and (2) access materials in Country A with the voluntary consent of a person who has lawful authority to disclose the materials. For advice regarding what constitutes voluntary consent or lawful authority for such disclosures, contact CCIPS.

Under certain circumstances, such as where the matter under consideration constitutes a violation of the foreign country's criminal law, foreign law enforcement authorities may be able to share evidence informally with U.S. counterparts. However, finding the appropriate official in Country A with which to explore such cooperation is an inexact science, at best. Possible avenues for entree to foreign law enforcement are: (1) the designated expert who participates in the G8's network of international high-tech crime points of contact (discussed below); (2) CCIPS's high-tech law enforcement contacts in many countries that are not a part of that network; (3) law enforcement contacts maintained by OIA; (4) representatives of U.S. law enforcement agencies who are stationed at the relevant American embassy (*e.g.*, FBI Legal Attaches, or "LegAtts," and agents from the U.S. Secret Service and U.S. Immigration and Customs Enforcement); and (5) the Regional Security Officer (from the Diplomatic Security Service) at the American embassy (who may have good in-country law enforcement contacts). CCIPS can be reached at 202-514-1026; OIA can be reached at 202-514-0000.

Where Country A cannot otherwise provide informal assistance, requests for evidence usually will be made under existing Mutual Legal Assistance Treaties (MLATs) or Mutual Legal Assistance Agreements, or through the Letters Rogatory process. *See* 28 U.S.C. §§ 1781-1782. These official requests for assistance are made by OIA to the designated "Central Authority" of Country A or, in the absence of an MLAT, to other appropriate authorities. (Central Authorities are usually located within the Justice Ministry, or another Ministry or office in Country A that has law enforcement authority.) OIA has attorneys responsible for every country and region of the world. Since official requests of this nature require specified documents and procedures and can take some time to produce results, law enforcement should contact OIA as soon as a request for international legal assistance becomes a possibility.

When U.S. law enforcement has reason to believe that electronic evidence exists on a computer or computer network located abroad, a request to foreign law enforcement for preservation of the evidence should be made as soon as possible. Such a request, similar to a request under 18 U.S.C. § 2703(f) to a U.S. provider (*see* Chapter 3.G.1), will have varying degrees of success based on several factors, most notably whether Country A has a data preservation law and whether the U.S. has sufficient law enforcement contacts in Country A to ensure prompt execution of the request. The International Convention on Cybercrime, completed in 2001, obligates all Parties to have the ability to effect cross-border preservation requests, and the availability of this critical form of assistance therefore is expected to increase greatly in the near future. Significantly, many countries do not have preservation and, if they receive a preservation request, will instead do a search. Such a search may not be appropriate for some cases; for example, it may risk tipping off the target of the investigation. Investigators may consult with CCIPS regarding the likely outcome of such a preservation request.

To secure preservation, or in emergencies when immediate international assistance is required, the international Network of 24-hour Points of Contact established by the High-tech Crime Subgroup of the G8 countries can provide assistance. This network, created in 1997, is comprised of approximately fifty member countries and continues to grow every year. Participating countries have a dedicated computer crime expert and a means to contact that office or person twenty-four hours a day. CCIPS is the point of contact for the United States and can be contacted at 202-514-1026 during regular business hours or at other times through the Department of Justice Command Center at 202-514-5000. The Council of Europe's Cybercrime Convention obligates all Parties to have a 24-hour point of contact for cybercrime cases, and international 24-hour response capabilities are therefore expected to continue to increase. The G8 and Council of Europe lists will be consolidated.

In the event that United States law enforcement inadvertently accesses a computer located in another country, CCIPS, OIA, or another appropriate authority should be consulted immediately, as issues such as sovereignty and comity may be implicated. Likewise, if exigencies such as terrorist threats indicate that direct access by United States law enforcement to a computer located abroad is crucial, appropriate U.S. authorities should be consulted immediately.

Searching, seizing, or otherwise obtaining electronic evidence located outside of the United States can raise difficult questions of both law and policy. For example, the Fourth Amendment may apply under certain circumstances, but not under others. *See generally United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990) (considering the extent to which the Fourth Amendment applies to searches outside of the United States). This manual does not attempt to provide detailed guidance on how to resolve difficult international issues that may arise in cases involving electronic evidence located beyond our borders. Investigators and prosecutors should contact CCIPS or OIA for assistance in particular cases.